TP-LINK®

150M 无线宽带路由器

TL-WR740N

详细配置指南

REV: 3.0.0
1910040154

声明

目 录

第1章 详细配置指南简介

本文档旨在帮助您正确使用路由器的功能，内容包括路由器的性能特征以及所有功能的详细说明。若要使用路由器中的其他应用方面的功能，可以参考本文档相关部分内容。

1.1 本书约定

1. 用"→"符号说明在 WEB 界面上的操作引导，其方法是点击菜单、选项、按钮等。
2. 路由器配置界面的菜单或按钮名采用**加粗**字表示，其它选项名或操作项等用""表示。
3. 图片界面都配有相关参数，这些参数主要是为正确配置产品参数提供参考。实际产品的配置界面并没有提供，请根据实际需要设置这些参数。

1.2 本书章节安排

第一章：详细配置指南简介。介绍本文档结构和编写约定。

第二章：产品概述。介绍路由器及其特性。

第三章：硬件描述。介绍路由器的前后面板以及安装环境注意事项。

第四章：快速安装指南。介绍硬件连接方法，并设置相关参数实现共享上网。

第五章：配置指南。介绍路由器包含的功能，请根据需要查看相关部分内容。

- QSS 安全设置：若您购买的 802.11n 无线网卡支持 WPS，可以通过 QSS 安全设置与网卡进行更为便捷和安全的无线连接。
- 网络参数：设置路由器的 LAN、WAN 口参数。LAN 口参数决定了计算机 IP 地址，正确设置计算机 IP 地址才能正常访问路由器；WAN 口参数直接影响是否可以上网，请根据网络服务提供商提供的参数正确设置。
- 无线参数：设置路由器的无线参数。只有当网卡的参数和路由器的参数相匹配时，才能正常使用无线功能访问路由器；同时，通过此功能给无线网络加密可以防止他人非法入侵无线网络。
- DHCP 服务器：此功能可以自动为计算机分配 IP 地址，无须手动设置计算机 IP 地址。
- 转发规则：当您将计算机设置成网络服务器后，请配置此功能以保证网络中的其他用户可以访问服务器。
- 安全设置：此功能可以限制外网向局域网发起的连接、抑制局域网的泛洪攻击，并可以设置路由器的 LAN、WAN 口的管理权限。
- 路由功能：对网络拓扑充分了解后，使用此功能可以减少路由选路造成的网络开销，提高数据包的转发速度。
- IP 带宽控制：此功能可以对局域网计算机上网带宽进行分配和控制，充分利用带宽资源，防止个别用户恶意抢占带宽。
- IP 与 MAC 绑定：此功能可以有效防止 ARP 攻击，维护局域网用户的上网安全。
- 动态 DNS：此功能可以使互联网计算机通过域名访问路由器或局域网中的服务器。

- 系统工具：此部分为维护路由器的系统操作工具，可以对路由器进行升级，查看路由器的配置信息，同时可通过恢复出厂设置将路由器恢复到出厂默认设置。

附录 A　FAQ：解决配置路由器过程中的常见问题。

附录 B　IE 浏览器设置：介绍如何设置 IE 浏览器，保证您正常访问路由器和上网。

附录 C　MAC 地址查询：介绍如何查看本机的 MAC 地址。

附录 D　规格参数：介绍路由器的详细规格参数。

第2章 产品概述

2.1 产品简介

为了充分利用该款路由器的各项功能，请仔细阅读该详细配置指南。

TL-WR740N 150M 无线宽带路由器是专为满足小型企业、办公室和家庭办公室的无线上网需要而设计的，它基于 IEEE 802.11n 标准，能扩展无线网络范围，提供最高达 150Mbps 的稳定传输，同时兼容 IEEE 802.11b 和 IEEE 802.11g 标准，功能实用、性能优越、易于管理并且提供多重安全防护措施，可以有效保护用户的无线上网安全。

2.2 主要特性

- 提供一个 10/100M 以太网(WAN)接口，可接 xDSL Modem/Cable Modem/Ethernet
- 内部集成四口交换机，提供四个 10/100M 以太网(LAN)接口
- 支持最高达 150Mbps 的传输速率，具备速率自适应功能，可以自动调整无线传输速率
- 支持 64/128/152 位 WEP 加密，WPA/WPA2、WPA-PSK/WPA2-PSK 等加密与安全机制，可以保证数据在无线网络传输中的安全
- 支持 11b only、11g only、11n only、11bg mixed 和 11bgn mixed 等多种无线模式
- 支持 SSID 广播控制，有效防止 SSID 广播泄密
- 内置网络地址转换(NAT)功能，支持虚拟服务器、特殊应用程序和 DMZ 主机
- 内建 DHCP 服务器，同时可进行静态地址分配
- 支持 VPN 穿透
- 支持通用即插即用(UPnP)，符合 UPnP 标准的数据可顺利通过
- 支持动态 DNS 功能，能够为动态 IP 地址提供域名服务
- 内置静态路由功能，可以根据需要构建特殊网络拓扑
- 支持基于 MAC 地址的局域网 WEB 管理，可以有效地限制局域网中计算机对 WEB 管理页面的访问
- 支持 WEB 软件升级，可以免费获得路由器的最新软件
- 可以根据上网动作，自动或按时连通和断开网络连接
- 支持本地和远端 WEB 管理，全中文配置界面，配备简易安装向导(Wizard)
- 支持 QSS 快速安全设置

第3章 硬件描述

3.1 面板布置

3.1.1 前面板

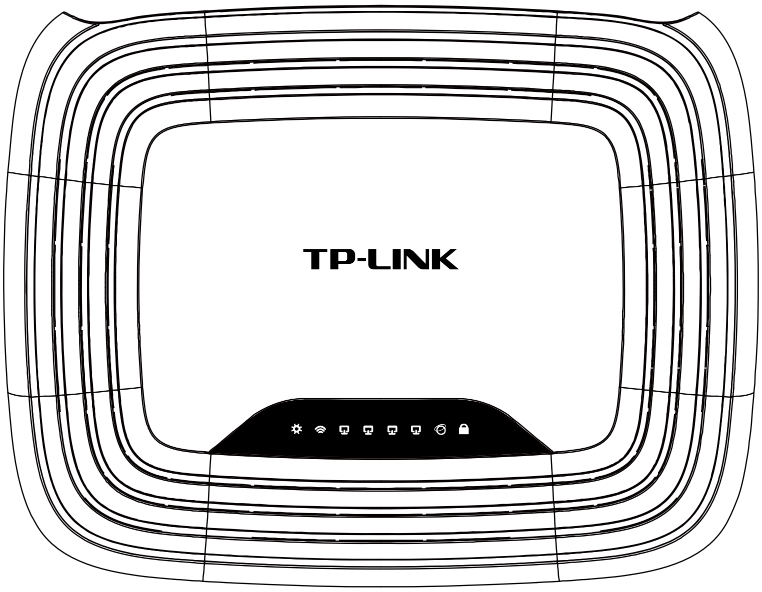


图 3-1 TL-WR740N 前面板示意图

指示灯：

指示灯	描述	功能
	系统状态指示灯	常灭－系统存在故障 常亮－系统初始化故障 闪烁－系统正常
	无线状态指示灯	常灭－没有启用无线功能 慢闪－已经启用无线功能 快闪－正在进行无线数据传输
	局域网状态指示灯	常灭－相应端口没有连接上 常亮－相应端口已正常连接 闪烁－相应端口正在进行数据传输
	广域网状态指示灯	常灭－端口没有连接上 常亮－端口已正常连接 闪烁－端口正在进行数据传输
	安全连接指示灯	慢闪－表示正在进行安全连接 此状态持续约 2 分钟 慢闪转为常亮－表示安全连接成功 慢闪转为快闪－表示安全连接失败

☞ 注意：

安全连接成功后，QSS 指示灯的常亮状态约持续 5 分钟后会自动熄灭，此种状态仍然属于正常连接状态。

3.1.2 后面板

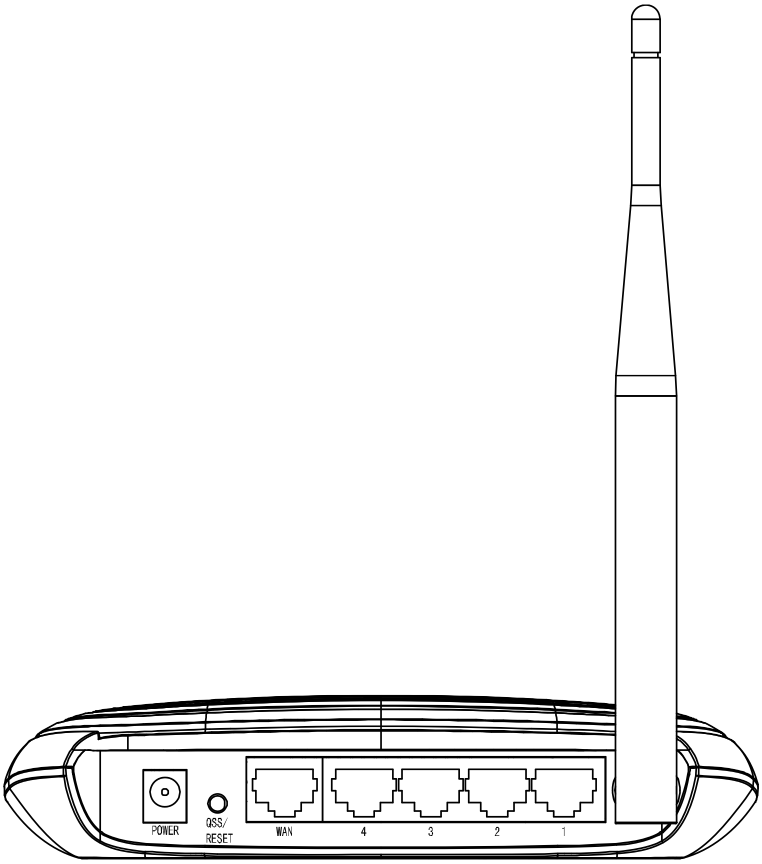


图 3-2 TL-WR740N 后面板示意图

1) **POWER**：用来连接电源，为路由器供电。

☞ 注意：

如果使用不匹配的电源，可能会导致路由器损坏。

2) **QSS/ RESET**：安全连接/复位按钮。短按时，启动快速安全连接功能，可用来与具备 WPS 功能的网络设备快速建立安全连接；长按超过 5 秒钟时，可使设备恢复到出厂默认设置。

3) **WAN**：广域网端口插孔(RJ45)。该端口用来连接以太网电缆或 xDSL Modem/Cable Modem。

4) **4/3/2/1**：局域网端口插孔(RJ45)。该端口用来连接局域网中的集线器、交换机或安装了网卡的计算机。

3.2 复位

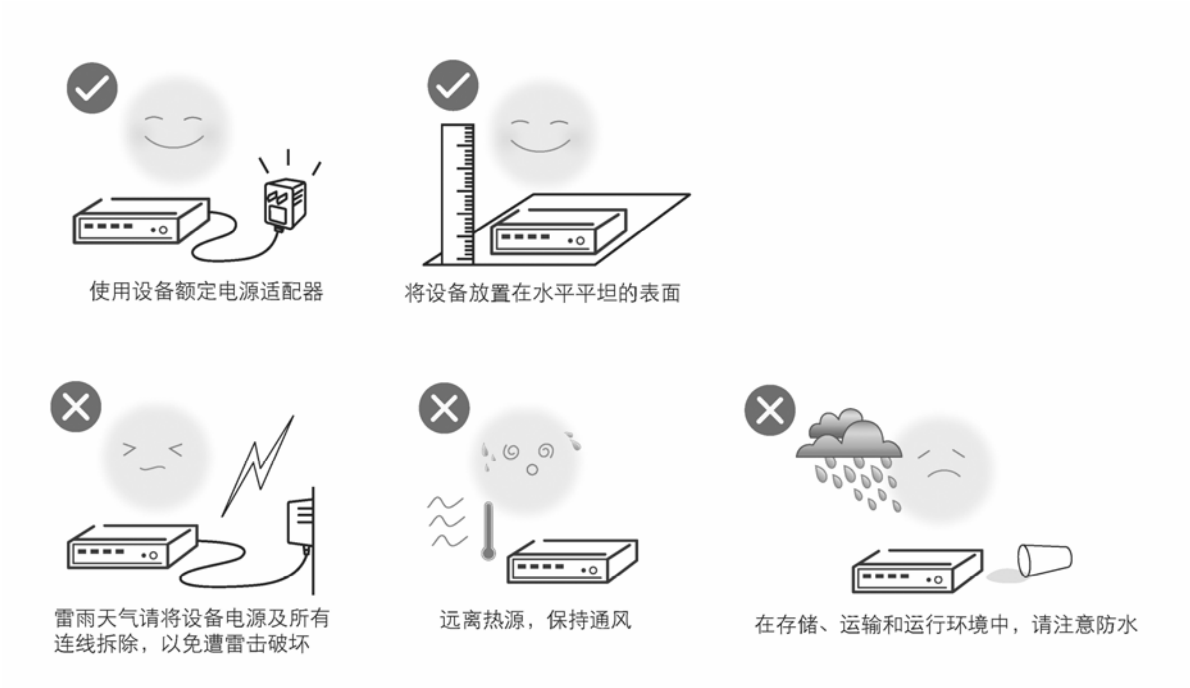
如果要将路由器恢复到出厂默认设置，请在路由器通电的情况下，按压 QSS/RESET 按钮，同时观察系统状态指示灯，大约等待五秒钟，当系统状态指示灯由缓慢闪烁变为快速闪烁状态时，表示路由器已成功恢复出厂设置，此时松开 QSS/RESET 按钮，路由器将重启。

3.3 系统需求

- 宽带 Internet 服务(接入方式为以太网电缆接入或通过 xDSL/Cable Modem 接入)
- 具有 RJ45 口的调制解调器(直接使用以太网电缆接入时不需要此设备)
- 每台 PC 的以太网连接设备(无线网卡或有线网卡及网线)
- 支持 TCP/IP 协议的操作系统
- Web 浏览器，如 Microsoft Internet Explorer、Mozilla Firefox、Apple Safari 等

3.4 安装环境

该路由器安装时应该遵循以下原则：



☞ 注意：

环境因素对传输距离有影响，详细介绍见附录A。

第4章 快速安装指南

本章介绍如何连接路由器并成功实现多台计算机共享上网。如果只进行基本配置，您只需阅读本章内容；如果要进行高级配置，请继续阅读第五章内容。

4.1 硬件连接

在安装路由器前，我们希望您已经能够利用宽带服务在单台计算机上成功上网。如果单台计算机上网有问题，请先和网络服务商（ISP）联系解决问题。当您成功地利用单台计算机上网后，请遵循以下步骤安装路由器。安装时请拔除电源插头，保持双手干燥。

1. 建立局域网连接

用网线将计算机直接连接到路由器LAN口，也可以将路由器的LAN口和局域网中的集线器或交换机通过网线相连，如下图 4-1所示。

2. 建立广域网连接

用网线将路由器WAN口和xDSL/Cable Modem或以太网相连，如下图 4-1所示。

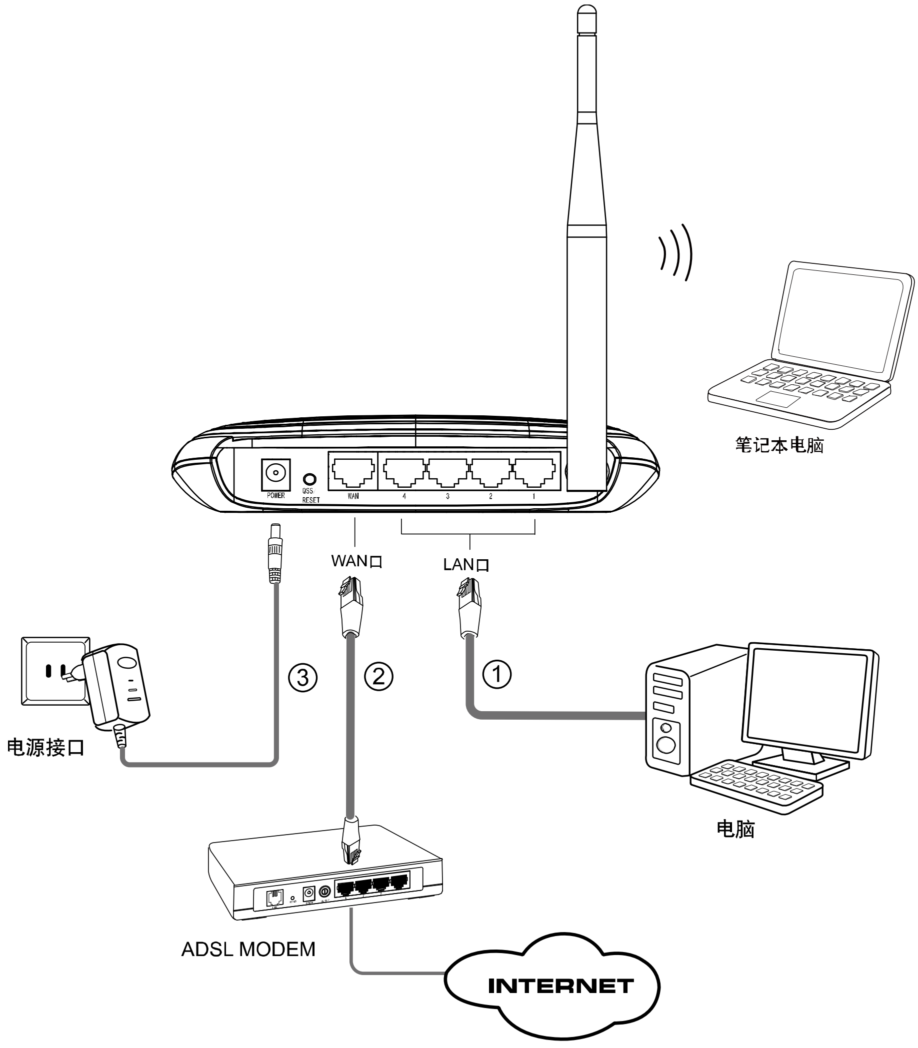


图 4-1 TL-WR740N 硬件安装示意图

3. 连接电源

连接好电源，路由器将自行启动。

4.2 建立正确的网络设置

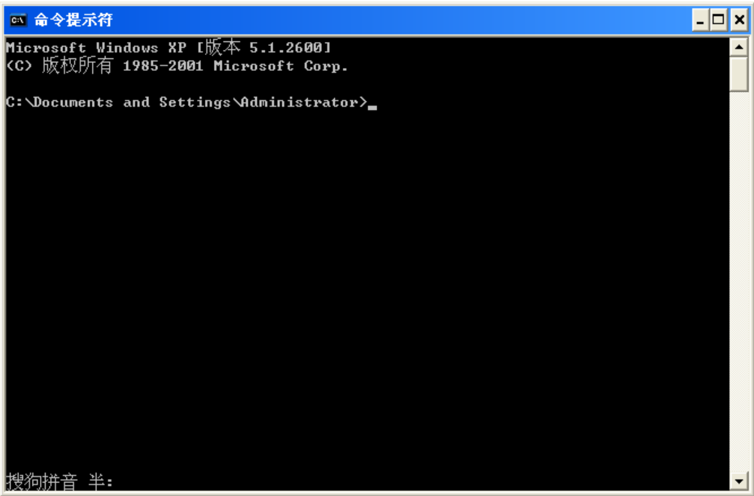
本路由器默认 LAN 口 IP 地址是 192.168.1.1，默认子网掩码是 255.255.255.0。这些值可以根据实际需要而改变，但本手册中将按默认值说明。本节以 Windows XP 系统为例，介绍计算机参数的设置步骤。

1. 右键单击桌面上的“网上邻居”图标，选择**属性**，在打开的“网络连接”页面中，右键单击“本地连接”，选择**状态**，打开“本地连接 状态”页面，然后按下图所示进行操作。

提示:

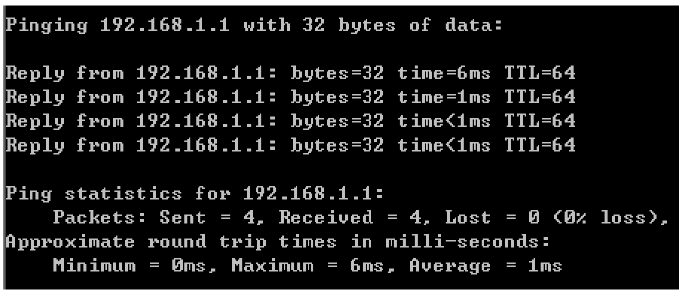
Windows 98 或更早版本的操作系统，以上设置可能需要重启计算机。

2. 使用 Ping 命令检查计算机和路由器之间是否连通。在 Windows XP 环境中，点击**开始－运行**，在随后出现的运行窗口输入“cmd”命令，回车或点击**确定**进入下图所示界面。



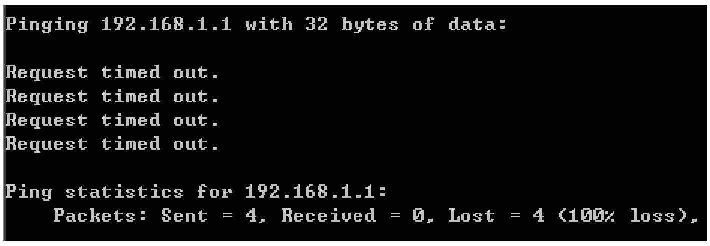
3. 输入命令：Ping 192.168.1.1，回车。

   如果屏幕显示为：



   计算机已与路由器成功建立连接。

   如果屏幕显示为：



这说明设备还未安装好，请按照下列顺序检查：

1) 硬件连接是否正确？

路由器面板上对应局域网端口的 Link/Act 指示灯和计算机上的网卡指示灯必须亮。

2) 计算机的 TCP/IP 设置是否正确？

若计算机的 IP 地址为前面介绍的自动获取方式，则无须进行设置。若手动设置 IP，请注意如果路由器的 IP 地址为 192.168.1.1，那么计算机 IP 地址必须为 192.168.1.X（X 是 2 到 254 之间的任意整数），子网掩码须设置为 255.255.255.0，默认网关须设置为 192.168.1.1。

4.3 快速安装指南

本产品提供基于WEB浏览器的配置工具。为了能顺利通过本路由器连接互联网，首先请设置WEB浏览器，具体设置步骤请参阅附录B IE浏览器设置。

打开网页浏览器，在浏览器的地址栏中输入路由器的IP地址：192.168.1.1，将会看到下图 4-2所示登录界面，输入用户名和密码（用户名和密码的出厂默认值均为**admin**），单击**确定**按钮。



图 4-2 登录界面

浏览器会弹出如下图 4-3所示的设置向导页面。如果没有自动弹出此页面，可以单击页面左侧的**设置向导**菜单将它激活。

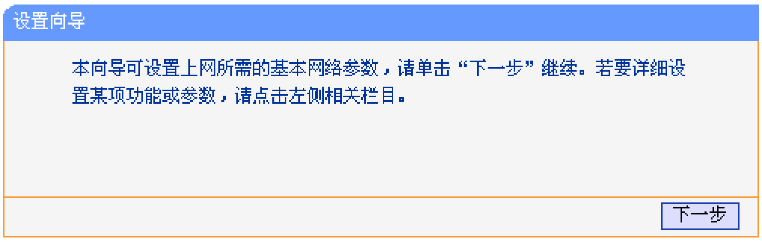


图 4-3 设置向导

单击**下一步**，进入下图 4-4所示的上网方式选择页面。

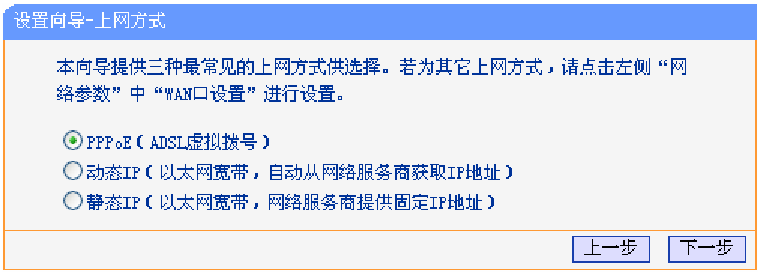


图 4-4 设置向导——上网方式

图 4-4显示了最常用的几种上网方式，请根据ISP提供的上网方式进行选择，然后单击**下一步**填写ISP提供的网络参数。

➢ **PPPoE（ADSL 虚拟拨号）**

如果您的上网方式为PPPoE，即ADSL虚拟拨号方式，ISP会给你提供上网帐号和口令，在下图 4-5所示页面中输入ISP提供的ADSL上网账号和口令。

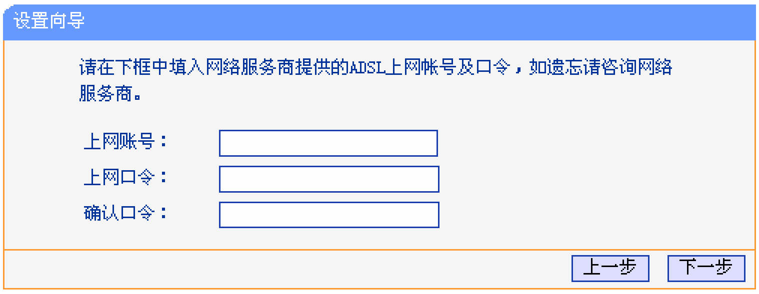


图 4-5 上网方式——PPPoE

➢ **动态IP（以太网宽带，自动从网络服务商获取IP地址）**

如果您的上网方式为动态IP，您可以自动从网络服务商获取IP地址，无须做任何设置。单击**下一步**转到图 4-7进行无线参数的设置。

➢ **静态 IP（以太网宽带，网络服务商提供固定 IP 地址）**

如果您的上网方式为静态IP，网络服务商会给您提供IP地址参数，您需要在下图 4-6所示页面中输入ISP提供的参数，若有不明白的地方请咨询网络服务商。



图 4-6 上网方式——静态 IP

IP 地址： 本路由器对广域网的 IP 地址，即 ISP 提供的 IP 地址，不清楚可以向 ISP 询问。

子网掩码： 本路由器对广域网的子网掩码，即 ISP 提供的子网掩码，一般为 255.255.255.0。

网关： 填入 ISP 提供的网关参数，不清楚可以向 ISP 询问。

DNS 服务器： 填入 ISP 提供的 DNS 服务器地址，不清楚可以向 ISP 询问。

备用 DNS 服务器：

可选项，如果 ISP 提供了两个 DNS 服务器地址，则可以把另一个 DNS 服务器地址的 IP 地址填于此处。

设置完成后，单击下一步，将看到下图 4-7所示的基本无线网络参数设置页面。

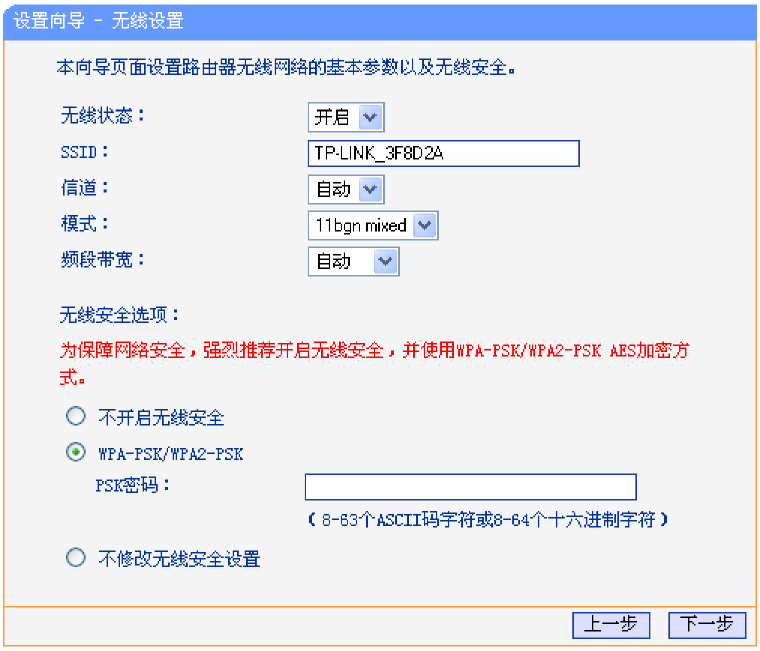


图 4-7 设置向导——无线设置

无线状态： 开启或者关闭路由器的无线功能。

SSID： 设置任意一个字符串来标明您的无线网络。

信道： 设置路由器的无线信号频段，推荐您选择自动。

模式： 设置路由器的无线工作模式，推荐您使用 11bgn mixed 模式。

频段带宽： 设置无线数据传输时所占用的信道宽度，可选项有：20M、40M 和自动。

不开启无线安全： 不开启无线安全功能，即不对路由器的无线网络进行加密，此时其他人均可以加入您的无线网络。

WPA-PSK/WPA2-PSK：

路由器无线网络的加密方式，如果选择了该项，请在 **PSK 密码**中输入您想要设置的密码，密码要求为 8-63 个 ASCII 字符或 8-64 个 16 进制字符。

不修改无线安全设置：

选择该项，则无线安全选项中将保持上次设置的参数。如果您从未更改过无线安全设置，则选择该项后，将保持出厂默认设置。

☞ 注意：

以上提到的信道带宽设置仅针对支持 IEEE 802.11n 协议的无线网络设备，对于不支持 IEEE 802.11n 协议的设备，此设置不生效。

设置完成后，单击**下一步**，如果您更改了无线设置，将弹出下图 4-8所示的设置向导完成界面，单击**重启**使无线设置生效。

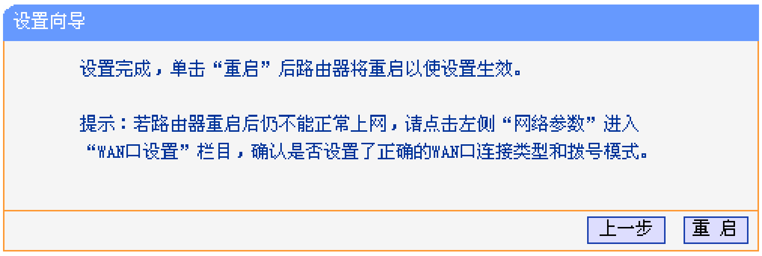


图 4-8 设置完成——重启使设置生效

第5章 配置指南

5.1 启动和登录

启动路由器并成功登录路由器管理页面后，在左侧菜单栏中，共有如下几个菜单：**运行状态**、**设置向导**、**QSS 安全设置**、**网络参数**、**无线设置**、**DHCP 服务器**、**转发规则**、**安全设置**、**路由功能**、**IP 带宽控制**、**IP 与 MAC 绑定**、**动态 DNS** 和**系统工具**。单击某个菜单项，即可进行相应的功能设置。下面将详细讲解各个菜单的功能。

5.2 运行状态

选择菜单**运行状态**，可以查看路由器当前的状态信息，包括LAN口状态、无线状态、WAN口状态和WAN口流量统计信息，如图 5-1。

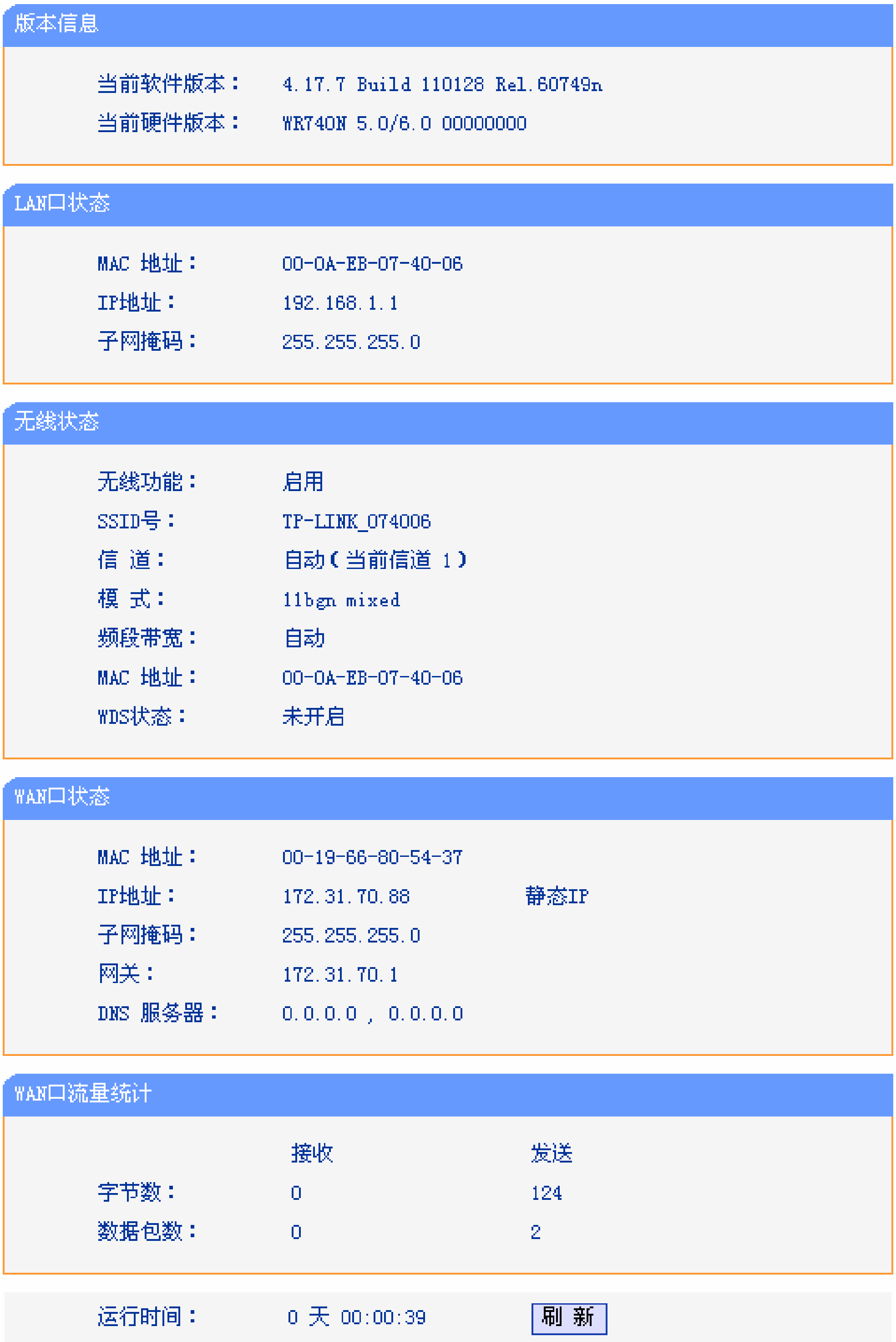


图 5-1 运行状态

版本信息： 此处显示路由器当前的软硬件版本号。您可以在**系统工具→软件升级**界面升级软件版本。

LAN口状态： 此处显示路由器当前LAN口的MAC地址、IP地址和子网掩码。其中IP地址和子网掩码可以在**网络参数→LAN口设置**界面中进行设置。

无线状态： 此处显示路由器当前的无线设置状态，包括 SSID、信道和频段带宽等信息。您可以在**无线设置→基本设置**界面进行相关设置。

WAN 口状态： 此处显示路由器当前 WAN 口的 MAC 地址、IP 地址、子网掩码、网关和 DNS 服务器地址。您可以在**网络参数→WAN 口设置**界面中进行相关设置。

5.3 设置向导

详见《无线宽带路由器用户手册》。

5.4 QSS安全设置

选择菜单QSS，可以在下图 5-2界面中进行快速无线安全设置。

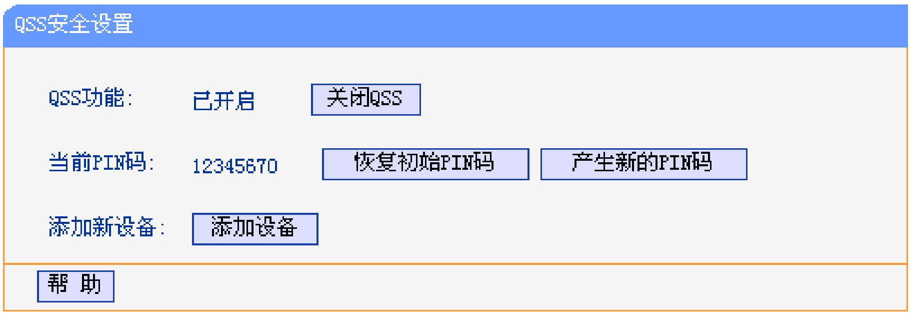


图 5-2 QSS 安全设置

QSS 功能： QSS 即快速安全设置，您可以使用该功能快速建立与无线网卡之间的无线连接。默认状态为开启。

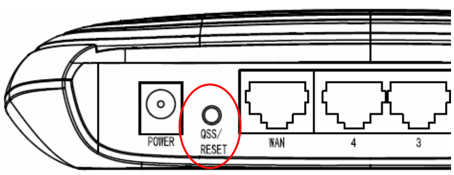
当前PIN码： PIN码即个人识别码，用于标识一件无线产品。PIN码可以更改，如果目前使用的PIN码与他人重复，可以点击**产生新的PIN码**，也可以点击**恢复初始PIN码**返回到最初PIN码值，恢复初始PIN码或者产生新的PIN码，都必须重启路由器后才能生效。

添加新设备： 点击**添加设备**进入添加新设备界面，在此界面可以手动配置路由器，添加要与其进行连接的无线设备。

QSS（Quick Secure Setup）能够快速建立与无线网卡之间的安全连接。如果您现在拥有支持 WPS（WiFi Protected Setup）的无线网卡，以我司 TL-WN821N 的 11N 无线 USB 网卡为例，您可以通过下面任意一种方法快速组建安全的无线网络：

方法一：

1. 按下路由器面板上的QSS快速安全按钮。



2. 接着按下网卡上的QSS快速安全按钮2到3秒不放。



3. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。

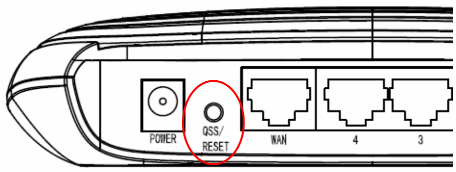


4. 出现下图所示界面则表示网卡端快速安全连接配置成功，单击**完成**结束配置。

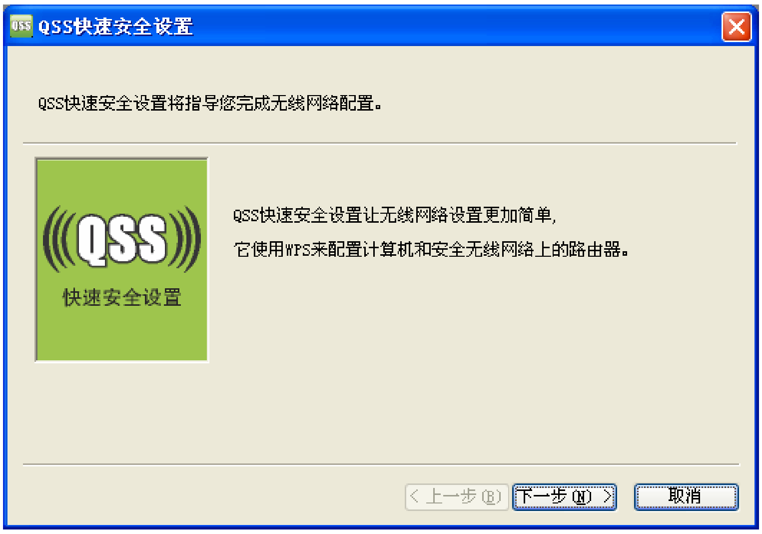


方法二：

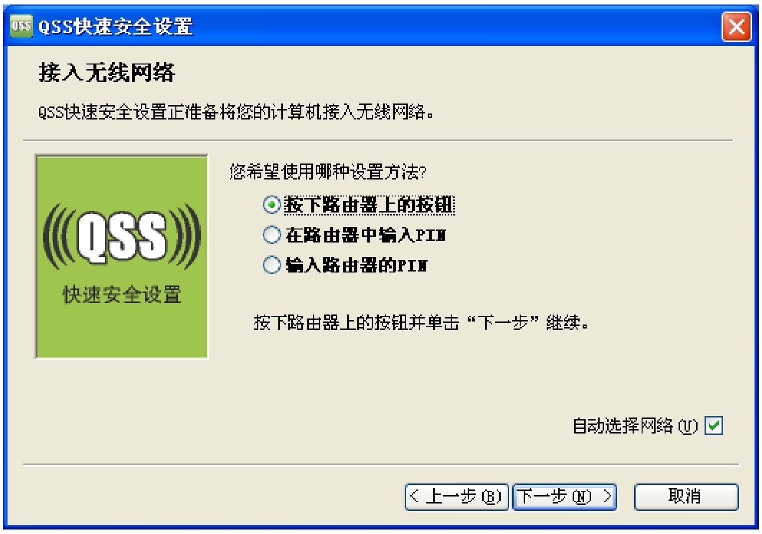
1. 按下路由器面板上的QSS快速安全按钮。



2. 进入网卡QSS软件配置界面（如下图），单击**下一步**。



3. 在随后出现的如下图所示的界面中选择第一项，单击**下一步**。



4. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。

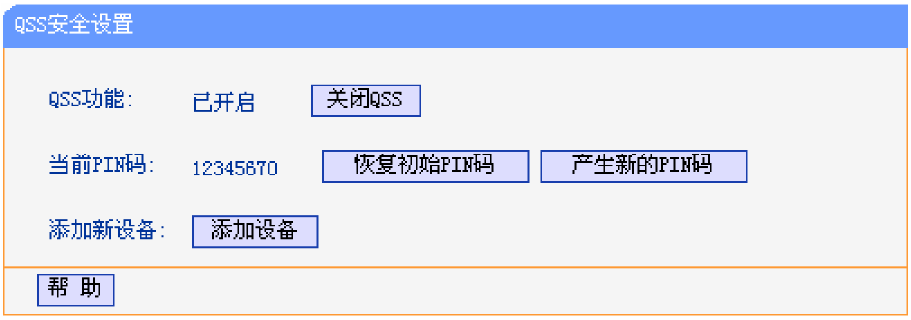


5. 出现下图所示界面则表示快速安全连接配置成功，单击**完成**结束配置。

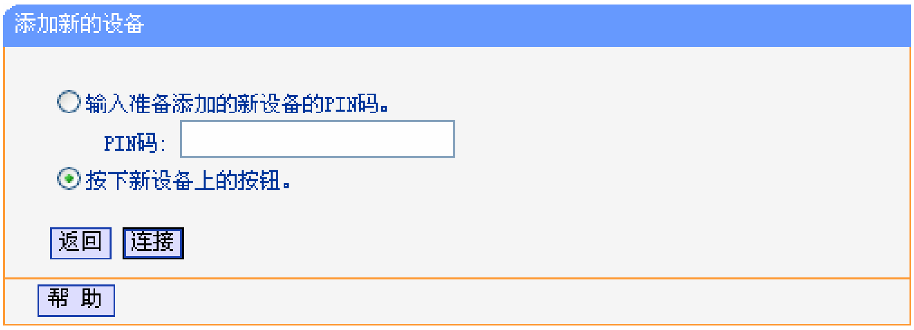


方法三：

1. 进入本路由器管理界面，在"QSS 安全设置"界面中（如下图）选择**添加设备**。



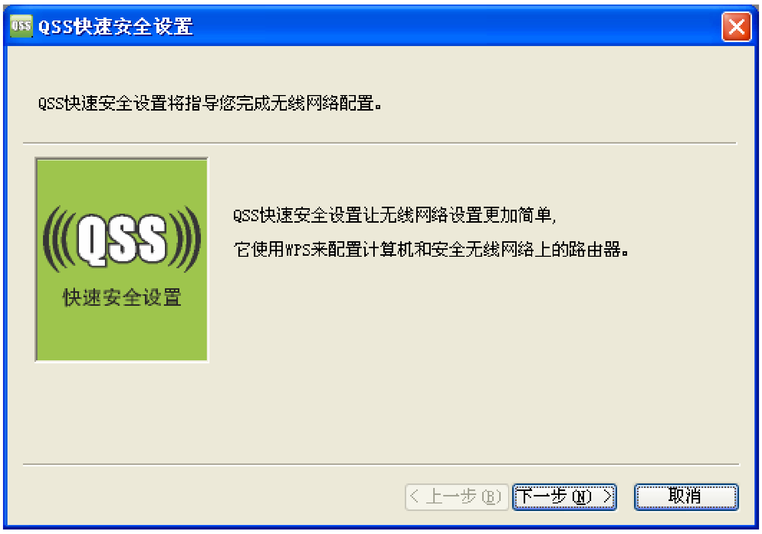
2. 在随后出现的如下图所示的界面中选择"按下新设备上的按钮"，然后点击**连接**按钮。



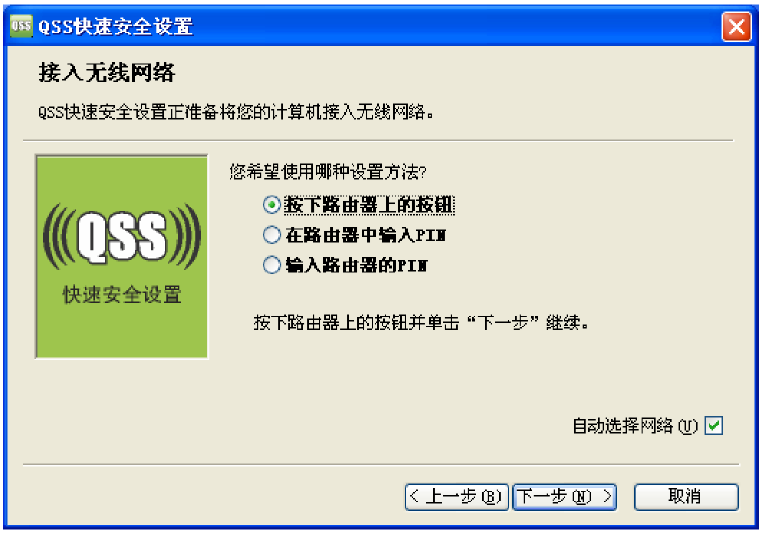
☞ 注意：

上述操作步骤 2 等同于按下路由器面板上的 QSS 快速安全按钮。

3. 进入网卡QSS软件配置界面（如下图），单击**下一步**。



4. 在随后出现的如下图所示的界面中选择第一项，单击**下一步**。



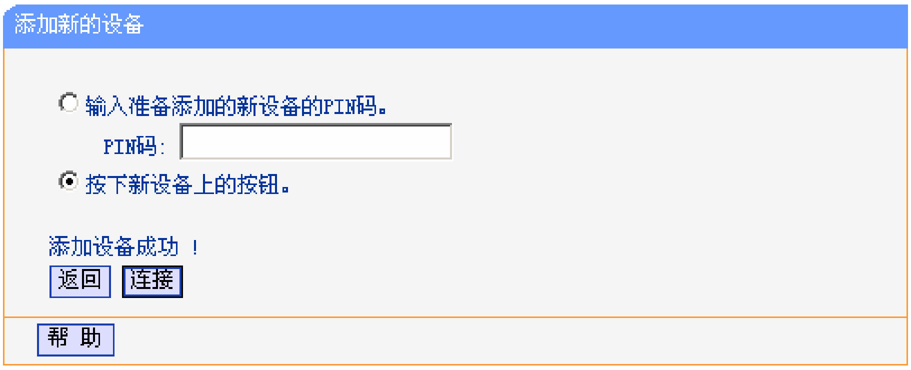
5. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。



6. 出现下图所示界面则表示网卡端快速安全连接配置成功，单击**完成**结束配置。

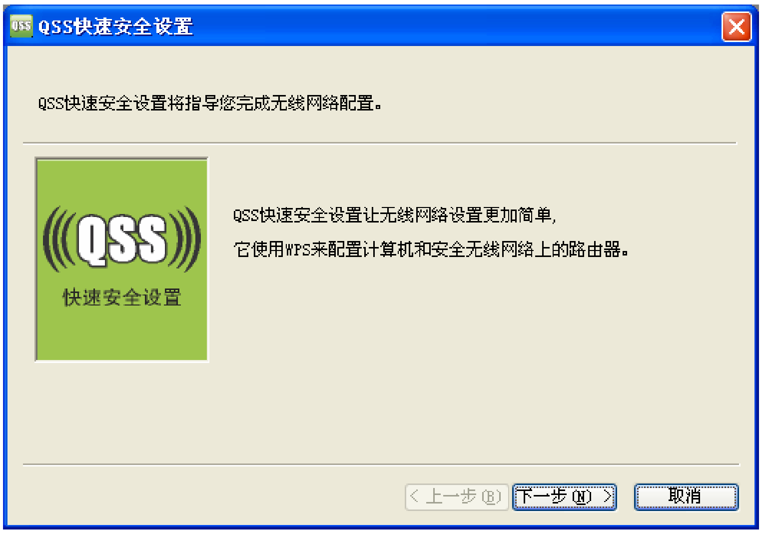


此时路由器端 QSS 安全设置的"添加新的设备"界面显示"添加设备成功"。



方法四：

1. 进入网卡QSS软件配置界面（如下图），单击下一步。



2. 在随后出现的如下图所示的界面中选择最后一项，并在"路由器 PIN"后面的方框中输入路由器底部标贴上的 8 位 PIN 码，单击下一步。

☞ 注意：

如果路由器已经有新的 PIN 码时，请您在路由器管理界面的"QSS 安全设置"界面中读取当前 PIN 码填在下图中的"路由器 PIN"后面的方框中。



3. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。

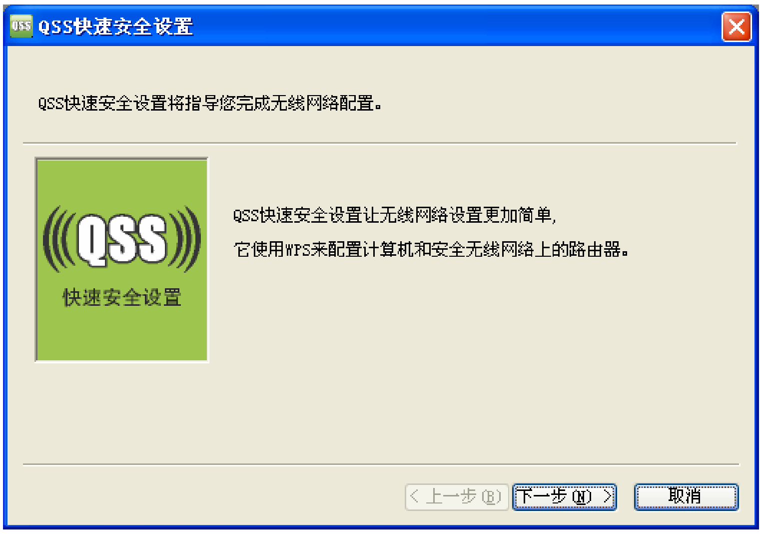


4. 出现下图所示界面则表示快速安全连接配置成功，单击**完成**结束配置。



方法五：

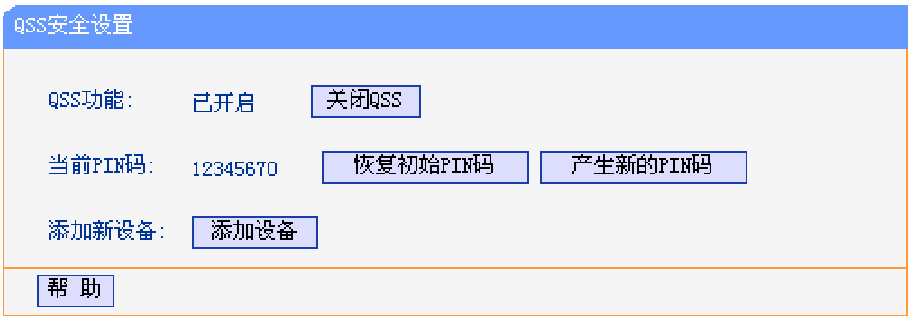
1. 进入网卡QSS软件配置界面（如下图），单击**下一步**。



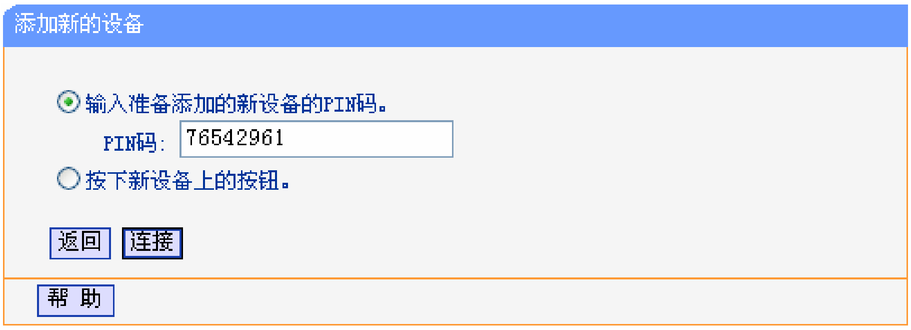
2. 在随后出现的如下图所示的界面中选择第二项，记录粗体显示的8位数字，这便是网卡的PIN码。然后单击**下一步**。



3. 进入本路由器管理界面，在"QSS 安全设置"界面中选择**添加设备**。



4. 在随后出现的如下图所示的界面中选择"输入准备添加的新设备的 PIN 码"，在下方的 PIN 码框中输入在第 2 步记录的 8 位网卡 PIN 码，然后点击**连接**按钮。



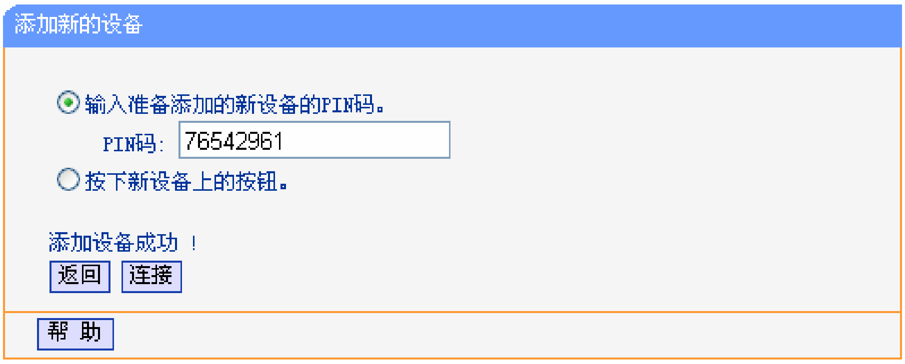
5. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。



6. 出现下图所示界面则表示网卡端快速安全连接配置成功，单击**完成**结束配置。



此时路由器端 QSS 安全设置的“添加新的设备”界面会显示“添加设备成功”。



5.5 网络参数

网络参数功能，可以根据组网需要设置路由器在局域网中的 IP 地址，并根据 ISP 提供的网络参数方便快捷地设置路由器 WAN 口参数，使局域网计算机能够共享 ISP 提供的网络服务。

选择菜单**网络参数**，可以看到：



单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.5.1 LAN口设置

在 LAN 口设置中，可以设置路由器的局域网 IP 地址和子网掩码，局域网用户可以通过此 IP 地址管理本路由器。若您为普通的家庭共享上网，则无须改变 LAN 口 IP 地址，保持默认值即可。

选择菜单**网络参数→LAN口设置**，可以在图 5-3界面中配置LAN接口的网络参数。

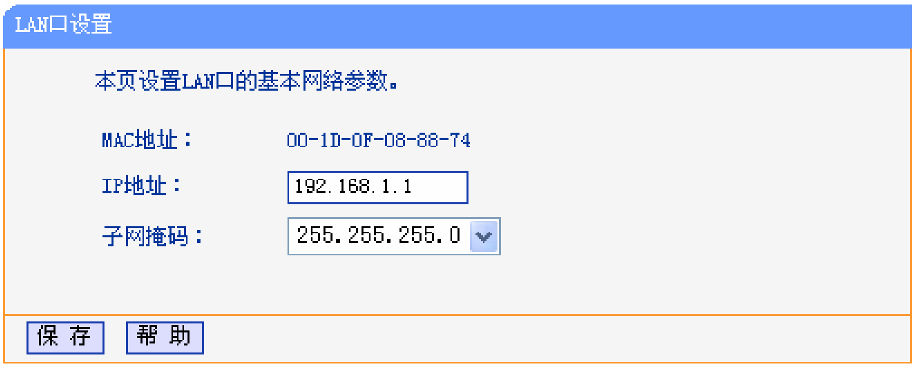


图 5-3 LAN 口设置

MAC地址： 本路由器对局域网的MAC地址，用来标识局域网。

IP地址： 输入本路由器对局域网的IP地址。局域网中所有计算机的IP地址必须与此IP地址处于同一网段且默认网关必须为此IP地址。该IP地址出厂默认值为192.168.1.1，为C类IP地址，适用于数量不超过200台计算机的小型网络，您可以根据组网需要改变它。

子网掩码： 选择路由器对局域网的子网掩码。C类IP地址对应子网掩码为255.255.255.0，为保证网络连接正常，请不要改变子网掩码。您可以根据实际的局域网类型以及IP地址类型选择不同的子网掩码。

完成更改后，点击**保存**按钮，路由器将自动重启以使现有设置生效。

☞ 注意：

1. 如果改变了本地IP地址，您必须用新的IP地址才能登录路由器的WEB管理界面，并且局域网中所有计算机的默认网关必须设置为该IP地址才能正常上网。
2. 局域网中所有计算机的子网掩码必须与此处子网掩码设置相同。

5.5.2 WAN口设置

WAN 是广域网(Wide Area Network)的缩写。在对 WAN 口参数的设置中，您可以根据 ISP 提供的连接类型方便快捷地设置路由器，使局域网计算机共享 ISP 提供的网络服务。在此设置中各种参数均由 ISP 提供，当参数不明确时请咨询 ISP。

选择菜单**网络参数→WAN口设置**，可以在随后出现的界面中配置WAN口的网络参数。本路由器支持3种上网方式：动态IP、静态IP和PPPoE，请咨询ISP提供哪种上网方式同时提供相关参数。

1. 动态 IP

当ISP未提供任何IP网络参数时，请选择**动态IP**。如图 5-4所示。选择**动态IP**，路由器将从ISP自动获取IP地址。

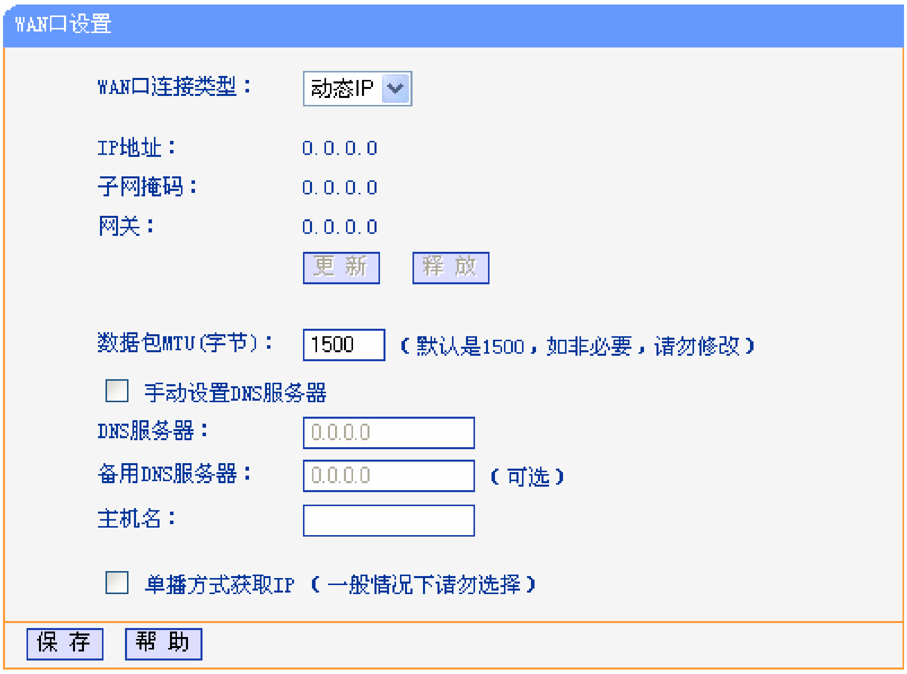


图 5-4 WAN 口设置-动态 IP

自动检测：	点击**自动检测**按钮，路由器能检测动态IP、静态IP和PPPoE三种上网方式，检测结果仅供参考，确切的上网方式请咨询ISP。
更新：	单击**更新**按钮，可以查看路由器从ISP的DHCP服务器上动态得到IP地址、子网掩码、网关以及DNS服务器。
释放：	单击**释放**按钮，路由器将发送DHCP释放请求给ISP的DHCP服务器，释放IP地址、子网掩码、网关以及DNS服务器设置。
数据包**MTU**：	MTU全称为最大数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。

DNS服务器、备用**DNS**服务器：

显示从ISP处自动获取的DNS服务器地址。当您需要使用已有的DNS服务器时，勾选"手动设置DNS服务器"，并在此处输入DNS服务器和备用DNS服务器(选填)的IP地址。路由器将优先连接手动设置的DNS服务器。

单播方式获取IP： 少数ISP的DHCP服务器不支持广播请求方式，如果您在网络连接正常的情况下无法获取IP地址，请选择此项。

完成更改后，点击**保存**按钮。

2. 静态 IP

当ISP提供的上网方式为静态IP时，ISP会提供上网账号和上网口令。IP地址、子网掩码、网关和DNS服务器等WAN IP信息时，请选择**静态IP**。如图 5-5所示。具体设置时，若不清楚，请咨询ISP。



图 5-5 WAN 口设置-静态 IP

自动检测： 点击**自动检测**按钮，路由器能检测动态IP、静态IP和PPPoE三种上网方式，检测结果仅供参考，确切的上网方式请咨询ISP。

IP地址： 输入ISP提供的IP地址信息，必填项。

子网掩码： 输入ISP提供的子网掩码，必填项。根据不同的网络类型子网掩码不同，一般为255.255.255.0(C类)。

网关： 输入ISP提供的网关参数。

数据包MTU： MTU全称为最大数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。

DNS服务器、备用DNS服务器：

ISP一般至少会提供一个DNS(域名服务器)地址，若提供了两个DNS地址则将其中一个填入"备用DNS服务器"栏。

完成更改后，点击**保存**按钮。

3. PPPoE

如果ISP提供的上网方式是PPPoE(以太网上的点到点连接)，ISP会提供上网账号和上网口令，请选择**PPPoE**。如图 5-6。具体设置时，若不清楚，请咨询ISP。

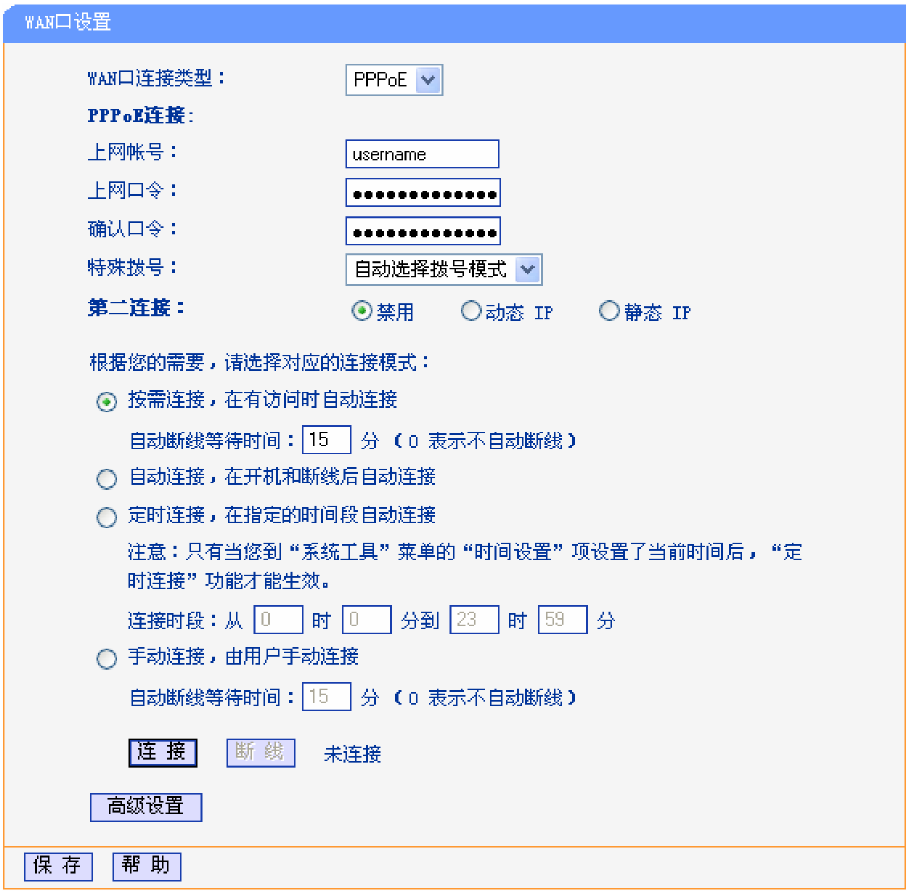


图 5-6 WAN 口设置-PPPoE

自动检测： 点击**自动检测**按钮，路由器能检测动态IP、静态IP和PPPoE三种上网方式，检测结果仅供参考，确切的上网方式请咨询ISP。

上网账号： 请正确输入ISP提供的上网账号，必须填写。

上网口令： 请正确输入ISP提供的上网口令，必须填写。

第二连接： 如果ISP还提供了以动态IP或静态IP的方式连接到局域网的连接，那么您可以相应地选择“动态IP”或“静态IP”来启动这个连接。

按需连接： 若选择按需连接模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行交费的用户，选择按需连接可以有效节省上网费用。

自动断线等待时间：

如果自动断线等待时间T不等于0(默认时间为15分钟)，则在检测到连续T分钟内没有网络访问流量时自动断开网络连接，保护上网资源。此项设置仅对“按需连接”和“手动连接”生效。

自动连接： 在开机后系统自动连接网络。在使用过程中，如果由于外部原因网络被断开，系统就会主动尝试连接，直到成功连接。若您的网络服务是包月交费形式，可以选择该项连接方式。

定时连接： 系统在连接时段的开始时刻主动进行网络连接，在终止时刻自动断开网络连接。选择此连接模式，可以有效控制内网用户的上网时间。

手动连接： 开机或断线后，您需要在此处或个人计算机中手动拨号连接。若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按时间交费，选择手动连接可有效节省上网费用。

连接/断线： 单击此按钮，可进行即时的连接/断线操作。

若需要进一步设置，可以点击**高级设置**按钮，在下图5-7界面中进行高级设置。

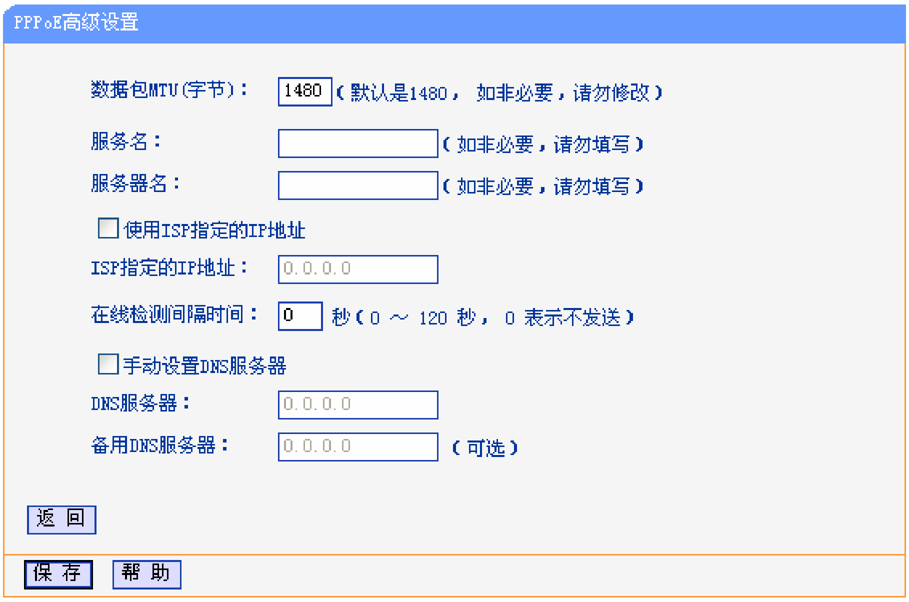


图 5-7 WAN 口设置-PPPoE-高级设置

数据包MTU： 填入网络数据包的MTU值，缺省为1480，如非特别需要，一般不要更改。

服务名、服务器名称：

如果不是ISP特别要求，请不要填写这两项。

使用ISP指定IP地址：

该项仅适用于静态PPPoE。如果ISP提供上网账号和口令时，还提供了IP地址，请选中此选择框，并输入PPPoE连接的静态IP地址。

在线检测间隔时间：

设置该值后，路由器将根据指定的时间间隔发送检测信号，以检测服务器是否在线。如果该值为0，则表示不发送检测信号。

DNS服务器、备用DNS服务器：

该处显示从ISP处自动获得的DNS服务器地址。当需要使用已有的DNS服务器时，请选择"手动设置DNS服务器"，并手动输入DNS服务器和备用DNS服务器IP地址(至少设置一个)。连接时，路由器将优先使用手动设置的DNS服务器。

完成更改后，点击**保存**按钮。

5.5.3 MAC地址克隆

选择菜单**网络参数→MAC地址克隆**，可以在下图 5-8界面中设置路由器对广域网的MAC地址。

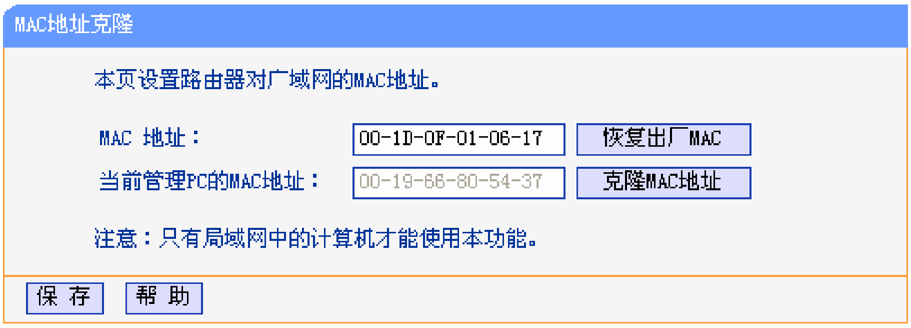


图 5-8 MAC 地址克隆

MAC地址： 此项默认为路由器WAN口的MAC地址。若ISP提供了一个MAC地址并要求对路由器WAN口的MAC地址进行绑定，只要将提供的值输入到“MAC地址”栏。除非ISP有特别要求，否则不建议更改MAC地址。

当前管理PC的MAC地址：

该处显示当前正在管理路由器的计算机的MAC地址。

恢复出厂MAC： 单击此按钮，即可恢复MAC地址为出厂时的默认值。

克隆MAC地址： 单击此按钮，可将当前管理PC的MAC地址克隆到“MAC地址”栏内。若ISP提供服务时要求进行MAC地址克隆，则应进行该项操作，否则无须克隆MAC地址。

完成更改后，点击**保存**按钮。

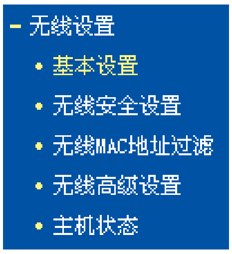
☞ 注意：

只有局域网中的计算机才能使用“MAC地址克隆”功能。

5.6 无线设置

无线设置功能，可以安全方便的启用路由器的无线功能进行网络连接。

选择菜单**无线设置**，可以看到：



单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.6.1 基本设置

基本设置可以开启并使用路由器的无线功能，组建内部无线网络。（组建网络时，内网主机需要无线网卡来连接到无线网络）但是此时的无线网络并不是安全的，建议您完成基本设置后进行相应的无线安全设置。

单击**基本设置**，可以在图 5-9中进行无线网络的基本设置。其中的SSID号和信道是路由器无线功能必须设置的参数。



图 5-9 无线网络基本设置

SSID 号： 即 Service Set Identification，用于标识无线网络的网络名称。您可以在此输入一个喜欢的名称，它将显示在无线网卡搜索到的无线网络列表中。

信道： 以无线信号作为传输媒体的数据信号传送的通道，选择范围从 1 到 13。如果您选择的是自动，则 AP 会自动根据周围的环境选择一个最好的信道。

模式： 该项用于设置路由器的无线工作模式，推荐使用 11bgn mixed 模式。

频段带宽： 设置无线数据传输时所占用的信道宽度，可选项为：20M、40M 和自动。

开启无线功能： 若要采用路由器的无线功能，必须选择该项，这样，无线网络内的主机才可以接入并访问有线网络。

开启 **SSID** 广播： 该项功能用于将路由器的 SSID 号向周围环境的无线网络内广播，这样，主机才能扫描到 SSID 号，并可以加入该 SSID 标识的无线网络。

开启 **WDS**： 可以选择这一项开启 WDS 功能，这个功能可以桥接多个无线局域网。注意：如果您开启了这个功能，最好要确保以下的信息输入正确。

桥接的 **SSID**： 要桥接的 AP 的 SSID。

桥接的 **BSSID**： 要桥接的 AP 的 BSSID。

扫描： 可以通过这个按钮扫描路由器周围的无线局域网。

密钥类型： 这个选项需要根据您桥接的 AP 的加密类型来设定，注意：最好情况下应该保持这个加密方式和 AP 设定的加密方式相同。

WEP 密钥序列号：

如果是 WEP 加密的情况，这个选项需要根据您桥接的 AP 的 WEP 密钥的序号来设定。

认证类型： 如果是 WEP 加密的情况，这个选项需要根据桥接的 AP 的认证类型来设定。

密钥： 根据桥接的 AP 的密钥设置来设置该项。

完成更改后，点击**保存**按钮并重启路由器使现在的设置生效。

☞ 注意：

1. 选择信道时请避免与当前环境中其他无线网络所使用的信道重复，以免发生信道冲突，使传输速率降低。
2. 以上提到的频段带宽设置仅针对支持IEEE 802.11n协议的网络设备；对于不支持IEEE 802.11n协议的设备，此设置不生效。例如，当本路由器与11N系列网卡客户端进行通信时频道带宽设置可以生效，当与11a/b/g系列网卡客户端进行通信时此设置将不再生效。
3. 当路由器的无线设置完成后，无线网络内的主机若想连接该路由器，其无线参数（如SSID号）必须与此处设置一致。

与路由器进行 WDS 连接的 AP，只需要工作在 AP 模式且支持 4 地址即可，不需要额外的配置。

5.6.2 无线安全设置

通过无线安全设置功能，可以防止他人未经同意私自连入您的无线网络，占用网络资源，同时也可以避免黑客窃听、黑客攻击等对您不利的行为，从而提高无线网络的安全性。

选择菜单**无线设置→无线安全设置**，可以在图 5-10界面中设置无线网络安全选项。

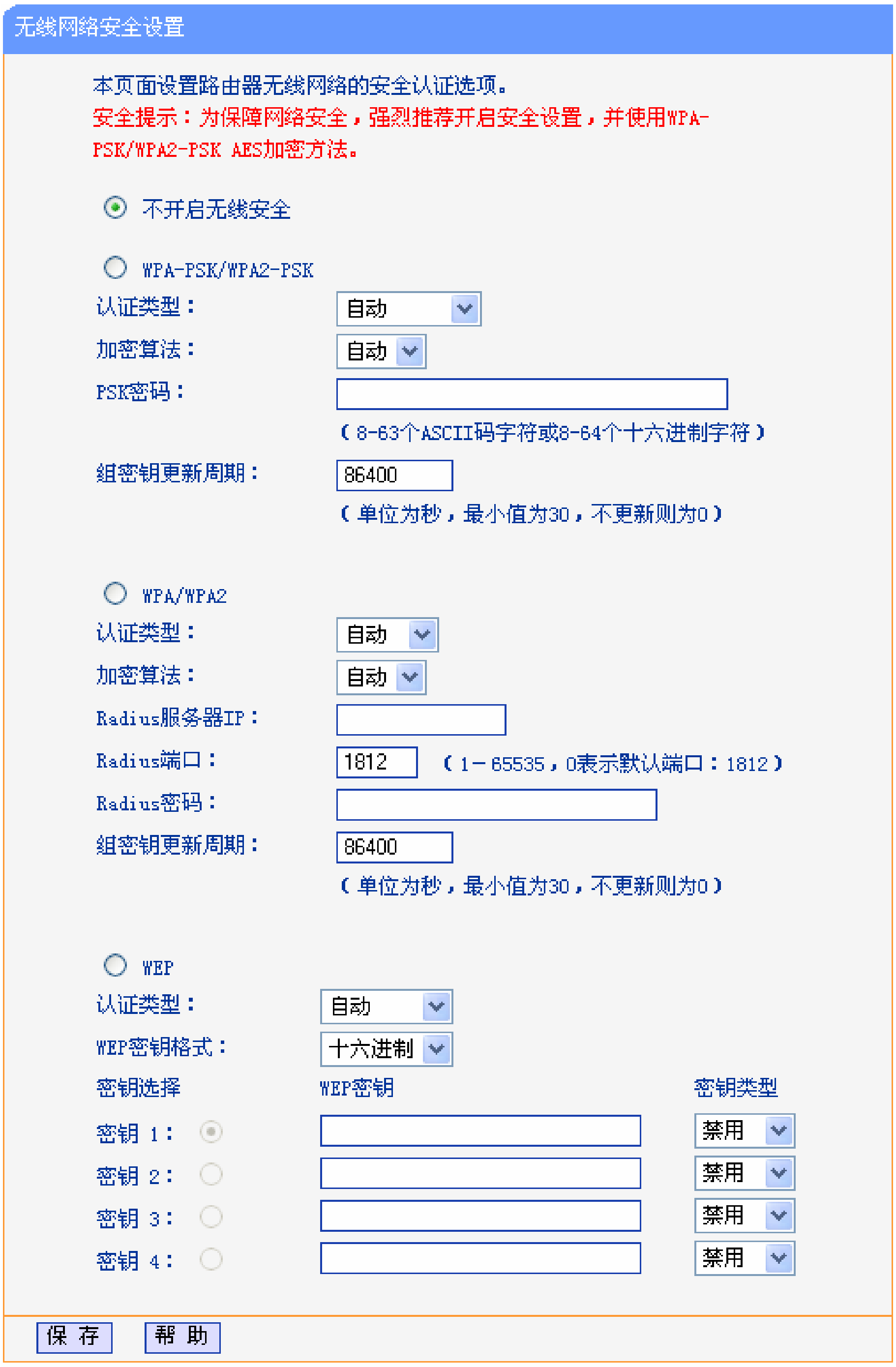


图 5-10 无线网络安全设置

在无线网络安全设置页面，可以选择是否关闭无线安全功能。

- 如果您无需开启无线安全功能，请勾选**关闭无线安全选项**以关闭无线安全功能。
- 如果您要开启无线安全功能，则请选择页面中三种安全类型中的一种进行无线安全设置。

本页面提供了三种无线安全类型：WPA-PSK/WPA2-PSK、WPA/WPA2 以及 WEP。不同的安全类型下，安全设置项不同，下面将详细介绍。

1. WPA-PSK/WPA2-PSK

WPA-PSK/WPA2-PSK安全类型其实是WPA/WPA2的一种简化版本，它是基于共享密钥的WPA模式，安全性很高，设置也比较简单，适合普通家庭用户和小型企业使用。其具体设置项见下图 5-11 示。



图 5-11 WPA-PSK/WPA2-PSK 安全模式

认证类型： 该项用来选择系统采用的安全模式，即自动、WPA-PSK、WPA2-PSK。

- 自动：若选择该项，路由器会根据主机请求自动选择WPA-PSK或WPA2-PSK安全模式。
- WPA-PSK：若选择该项，路由器将采用WPA-PSK的安全模式。
- WPA2-PSK：若选择该项，路由器将采用WPA2-PSK的安全模式。

加密算法： 该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为自动，选择该项后，路由器将根据实际需要自动选择TKIP或AES加密方式。注意11N模式不支持TKIP算法。

PSK密码： 该项是WPA-PSK/WPA2-PSK的初始设置密钥，设置时，要求为8-63个ASCII字符或8-64个十六进制字符。

组密钥更新周期： 该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为30，若该值为0，则表示不进行更新。

☞ 注意：

若路由器进行了无线安全设置，则该无线网络内的所有主机都必须根据此处的安全设置进行相应的设置，如密码设置必须完全一样，否则将不能成功的通过无线连接到该路由器。

2. WPA/WPA2

WPA/WPA2是一种比WEP强大的加密算法，选择这种安全类型，路由器将采用Radius服务器进行身份认证并得到密钥的WPA或WPA2安全模式。由于要架设一台专用的认证服务器，代价比较昂贵且维护也很复杂，所以不推荐普通用户使用此安全类型。其具体设置项见下图 5-12示。



图 5-12 WPA/WPA2 安全模式

认证类型： 该项用来选择系统采用的安全模式，即自动、WPA、WPA2。

- 自动：若选择该项，路由器会根据主机请求自动选择WPA或WPA2安全模式。
- WPA：若选择该项，路由器将采用WPA的安全模式。
- WPA2：若选择该项，路由器将采用WPA2的安全模式。

- 加密算法：该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为自动，选择该项后，路由器将根据实际需要自动选择TKIP或AES加密方式。这里需要注意的是，当您选择WPA/WPA2 TKIP加密时，由于802.11N不支持此加密方式，所以路由器可能工作在较低的传输速率上，建议使用WPA2-PSK等级的AES加密。如图 5-13。

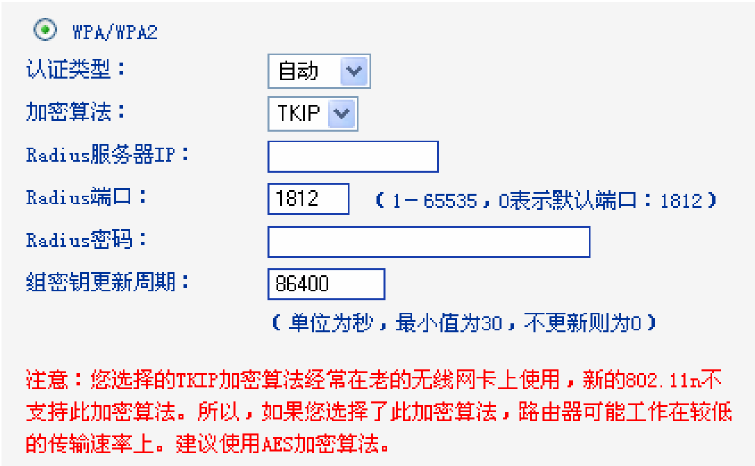


图 5-13 选择 WPA/WPA2 TKIP 加密

Radius服务器IP： Radius服务器用来对无线网络内的主机进行身份认证，此项用来设置该服务器的IP地址。

Radius端口： Radius服务器用来对无线网络内的主机进行身份认证，此项用来设置该Radius认证服务采用的端口号。

Radius密码： 该项用来设置访问Radius服务的密码。

组密钥更新周期： 该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为30，若该值为0，则表示不进行更新。

3. WEP

WEP是Wired Equivalent Privacy的缩写，它是一种基本的加密方法，其安全性不如另外两种安全类型高。选择WEP安全类型，路由器将使用802.11基本的WEP安全模式。这里需要注意的是因为802.11N不支持此加密方式，如果您选择此加密方式，路由器可能会工作在较低的传输速率上。其具体设置项见下图 5-14示。



图 5-14 WEP 安全模式

认证类型： 该项用来选择系统采用的安全模式，包括自动、开放系统、共享密钥。

- 自动：若选择该项，路由器会根据主机请求自动选择开放系统或共享密钥方式。
- 开放系统：若选择该项，路由器将采用开放系统方式。此时，无线网络内的主机可以在不提供认证密码的前提下，通过认证并关联上无线网络，但是若要进行数据传输，必须提供正确的密码。
- 共享密钥：若选择该项，路由器将采用共享密钥方式。此时，无线网络内的主机必须提供正确的密码才能通过认证，否则无法关联上无线网络，更无法进行数据传输。

WEP密钥格式： 该项用来选择即将设置的密钥的形式，包括16进制、ASCII码。若采用16进制，则密钥字符只能为0～9，A、B、C、D、E、F；若采用ASCII码，则密钥字符可以是键盘上的任意字符。

密钥选择、WEP密钥、密钥类型：

这三项用来选择密钥，设置具体的密钥值和选择密钥的类型，密钥的长度受密钥类型的影响。

密钥长度说明：选择64位密钥需输入16进制字符10个，或者ASCII码字符5个。选择128位密钥需输入16进制字符26个，或者ASCII码字符13个。选择152位密钥需输入16进制字符32个，或者ASCII码字符16个。

☞ 注意：

关于密钥选择中的4个密钥，可以只使用其一，也可以多个同时使用。无论哪种情况，客户端网卡上密钥的设置都必须与之一一对应。

5.6.3 无线MAC地址过滤

MAC 地址是网卡的物理地址，它就像是网卡的身份证，在网络中进行网卡的识别都是通过这个地址进行的。通常说的计算机的 MAC 地址也即计算机上网卡的 MAC 地址。

无线 MAC 地址过滤功能就是通过 MAC 地址来控制计算机能否接入无线网络，从而有效控制无线网络内用户的上网权限。

无线 MAC 地址过滤功能通过 MAC 地址允许或拒绝无线网络中的计算机访问广域网，有效控制无线网络内用户的上网权限。您可以点击按钮**添加新条目**来增加新的过滤规则；或者通过“编辑”、“删除”链接来编辑或删除列表中的过滤规则。

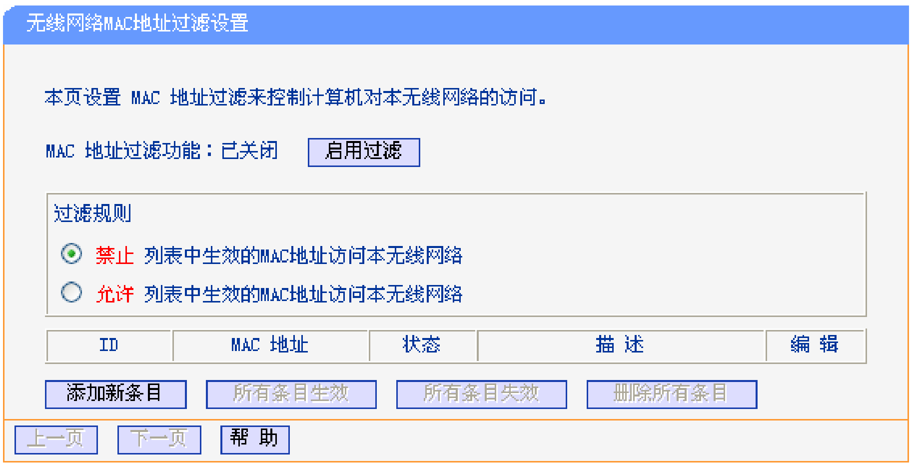


图 5-15 无线网络 MAC 地址过滤设置

MAC地址过滤功能：

请在该处选择是否开启路由器的无线网络MAC地址过滤功能。只有选择开启时，下面的设置才会生效。

过滤规则： 请选择MAC地址过滤规则，允许或禁止列表中生效规则之外的MAC地址所对应的计算机访问本无线网络。

点击**添加新条目**按钮后，可以在图 5-16界面中设置过滤规则条目：

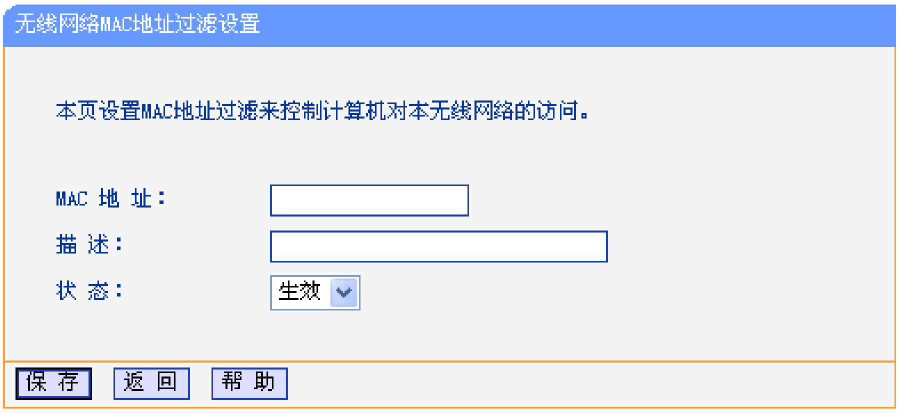


图 5-16 无线网络 MAC 地址过滤设置

MAC地址： 用于输入所管理的计算机的MAC地址。

状态： 用于设置MAC地址过滤条目的状态。"生效"表示该设置条目被启用，"失效"表示该设置条目未被启用。

描述： 对主机的简单描述，可选设置，但为了方便您识别不同的计算机，建议进行设置。

设置完成后，设置结果将显示在图5-15中列表当中。

举例：如果您想禁止MAC地址为"00-13-8F-A9-E6-CA"和"00-13-8F-A9-E6-CB"的主机访问您的无线网络，而其他主机可以访问此无线网络，请按照以下步骤进行配置：

1. 在上图5-15中，点击**启用过滤**按钮，开启无线网络的访问控制功能。
2. 在图5-15中，选择过滤规则为"允许列表中生效规则之外的MAC地址访问本无线网络"，并确认访问控制列表中没有任何你不需要过滤的MAC地址生效条目，如果有，将该条目状态改为"失效"或删除该条目，也可以点击**删除所有条目**按钮，将列表中的条目清空。
3. 在图5-15中，点击**添加新条目**按钮，按照下图5-17界面，设置MAC地址为"00-13-8F-A9-E6-CA"，状态为"生效"。设置完成后，点击**保存**按钮。

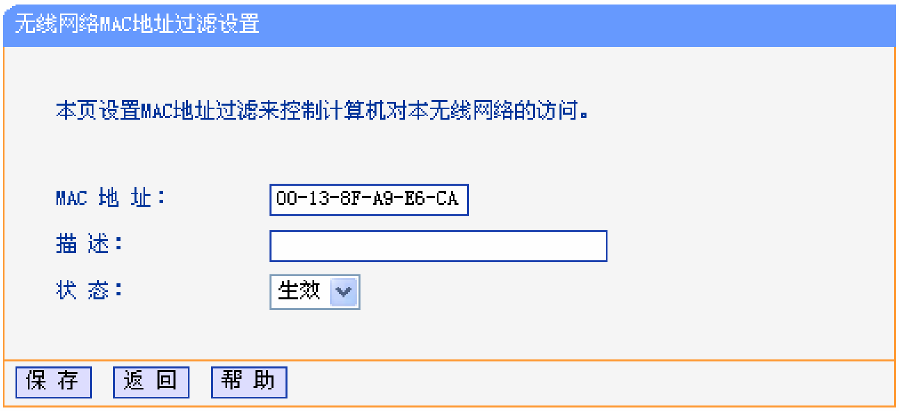


图 5-17 添加无线网络 MAC 地址过滤条目

4. 参照第三步，继续添加过滤条目，设置MAC地址为"00-13-8F-A9-E6-CB"，状态为"生效"。设置完成后，点击**保存**按钮。

例1中设置完成后生成的MAC地址过滤列表为：

ID	MAC地址	状态	描 述	编 辑
1	00-13-8F-A9-E6-CA	生效		编辑 删除
2	00-13-8F-A9-E6-CB	生效		编辑 删除

☞ 注意：

如果开启了无线网络的MAC地址过滤功能，并且过滤规则选择了“禁止列表中生效规则之外的MAC地址访问本无线网络”，而过滤列表中又没有任何生效的条目，那么任何主机都不可以访问本无线网络。

5.6.4 无线高级设置

此界面用于设置路由器的高级无线功能，建议这些操作由专业人员进行，因为不正确的设置可能会降低路由器的无线性能。

选择菜单**无线设置→无线高级设置**，可以看到如下图 5-18的无线高级设置界面。



图 5-18 无线高级设置

Beacon时槽： 路由器通过发送Beacon广播进行无线网络连接的同步。Beacon时槽表示路由器发送Beacon广播的频率。默认值为100毫秒。Beacon广播的取值范围是20－1000毫秒。

RTS时槽： 为数据包指定RTS（Request to Send，发送请求）阈值。当数据包长度超过RTS阈值时，路由器就会发送RTS到目的站点来进行协商。接收到RTS帧后，无线站点会回应一个CTS（Clear to Send，清除发送）帧来回应路由器，表示两者之间可以进行无线通信了。

分片阈值： 为数据包指定分片阈值。当数据包的长度超过分片阈值时，会被自动分成多个数据包。过多的数据包将会导致网络性能降低，所以分片阈值不应设置过低。当您在图 5-9界面中选择路由器的模式为11n（11n only 或11bgn mixed）时，此值不能改动。默认值为2346。

DTIM阈值： 该值在1至255之间，指定传输指示消息(DTIM)的间隔。DTIM是一种倒数计时作业，用以告知下一个要接收广播及多播的客户端窗口。当路由器已经为相关联的客户端缓存了广播或者多播信息时，它会在Beacon中夹带有下一个DTIM时槽的信息；当客户端听到Beacon讯号时，就会接收该广播和组播信息。默认值为1。

开启WMM： 开启WMM后路由器具有无线服务质量(QoS)功能，可以对音频、视频数据优先处理，保证音频、视频数据的优先传输。推荐您勾选此项。

开启Short GI： 选择此项可以使路由器接收和发送短帧间隔数据包，提高路由器的传输速率，推荐勾选。

开启AP隔离： 选择此项可以隔离关联到AP的各个无线站点。

完成更改后，点击**保存**按钮。

5.6.5 主机状态

此页面显示连接到本无线网络中的所有主机的基本信息。选择菜单**无线设置→主机状态**，可以在下图 5-19界面中查看当前连接到无线网络中的所有主机的基本信息。单击**刷新**按钮，可以更新列表中的条目信息。



图 5-19 无线网络主机状态

MAC地址： 显示当前已经连接到无线网络的主机的MAC地址。

当前状态： 显示当前主机的运行状态。

接收数据包数、发送数据包数：

显示当前主机接收和发送的数据包的总数。

5.7 DHCP服务器

DHCP，即 Dynamic Host Control Protocol，动态主机控制协议。TL-WR740N 有一个内置的 DHCP 服务器，可以实现局域网内的计算机 IP 地址的自动分配。

选择菜单 **DHCP 服务器**，可以看到：



单击菜单中的某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.7.1 DHCP服务

如果启用了DHCP服务功能，并将计算机获取IP的方式设为“自动获得IP地址”，则打开计算机时，DHCP服务器会自动从地址池中分配未被使用的IP地址到计算机，而不需要手动进行设置。

选择菜单**DHCP服务器→DHCP服务**，将看到DHCP设置界面，如图 5-20。



图 5-20 DHCP 服务

DHCP服务器： 选择是否启用DHCP服务器功能，默认为启用。

地址池开始/结束地址： 分别输入开始地址和结束地址。完成设置后，DHCP服务器分配给内网主机的IP地址将介于这两个地址之间。

地址租期： 即DHCP服务器给内网主机分配的IP地址的有效使用时间。在该段时间内，服务器不会将该IP地址分配给其它主机。

网关： 可选项。应填入路由器LAN口的IP地址，缺省为192.168.1.1。

缺省域名： 可选项。应填入本地网域名，缺省为空。

主/备用DNS服务器： 可选项。可以填入ISP提供的DNS服务器或保持缺省，若不清楚可咨询ISP。

完成更改后，点击**保存**按钮并重启路由器使设置生效。

☞ 注意：

若要使用本路由器的 DHCP 服务器功能：

1. 局域网中计算机获取 IP 的方式必须设置为“自动获得 IP 地址”,设置方法详见附录 X;
2. 必须事先指定 IP 地址池的开始和结束地址。

5.7.2 客户端列表

客户端列表显示当前所有通过 DHCP 服务器获得 IP 地址的客户端主机的相关信息，包括客户端名、MAC 地址、所获得的 IP 地址、及 IP 地址的有效时间。

选择菜单**DHCP服务器→客户端列表**，可以查看客户端主机的相关信息；单击**刷新**按钮可以更新表中信息，如图 5-21。

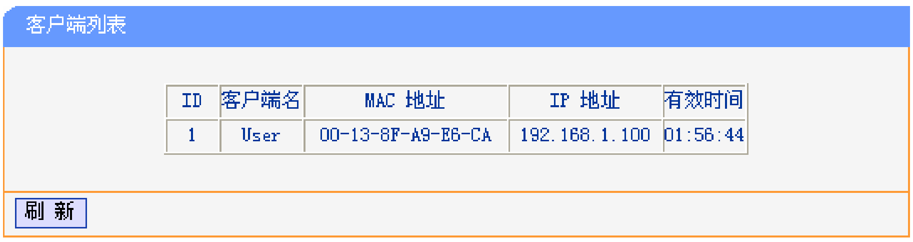


图 5-21 客户端列表

客户端名： 显示获得IP地址的客户端计算机的名称。

MAC地址： 显示获得IP地址的客户端计算机的MAC地址。

IP地址： 显示DHCP服务器分配给客户端主机的IP地址。

有效时间： 指客户端主机获得的IP地址距到期所剩的时间。每个IP地址都有一定的租用时间，客户端软件会在租期到期前自动续约。

5.7.3 静态地址分配

静态地址分配功能可以为指定MAC地址的计算机预留IP地址。当该计算机请求DHCP服务器分配IP地址时，DHCP服务器将给它分配表中预留的IP地址。

选择菜单**DHCP服务器→静态地址分配**，可以在下图 5-22所示界面中查看和编辑静态IP地址分配条目。



图 5-22 静态地址分配

点击**添加新条目**按钮，可以在图 5-23所示界面中设置新的静态地址分配条目。

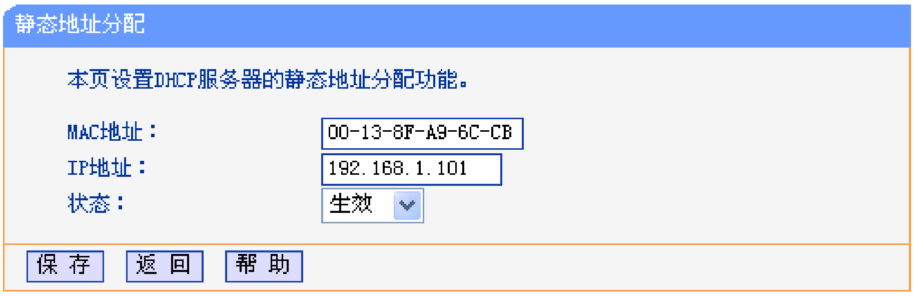


图 5-23 添加静态地址条目

MAC地址： 输入需要预留静态IP地址的计算机的MAC地址。

IP地址： 预留给内网主机的IP地址。

状态： 设置该条目是否生效。只有状态为生效时，本条目的设置才生效。

举例： 如果您希望给局域网中MAC地址为00-13-8F-A9-6C-CB的计算机预留IP地址192.168.1.101。这时请按照如下步骤设置：

1. 在图 5-22界面中单击**添加新条目**按钮。
2. 在图 5-23界面中设置MAC地址为“00-13-8F-A9-6C-CB”，IP地址为“192.168.1.101”，状态为“生效”。
3. 点击**保存**按钮，可以看到设置完成后的静态地址分配列表如图 5-22所示。
4. 重启路由器使设置生效。

5.8 转发规则

通过转发规则功能，可以使远程用户访问局域网计算机上的资源，还可以在局域网用户运行某些特殊应用程序（如 Internet 网络游戏、视频会议、网络电话）时，建立用户端与因特网服务器之间的连接。

选择菜单**转发规则**，可以看到：



单击菜单中的子项即可进行具体的设置，下面将详细讲解各子项的功能和设置方法。

5.8.1 虚拟服务器

通过将本路由器配置为虚拟服务器，可以使远程用户访问局域网内部的服务器，如 Web、FTP、邮件服务器等。

为保证局域网的安全，默认情况下，路由器会将局域网主机的 IP 地址隐藏起来，使因特网计算机无法主动与局域网计算机建立连接。因此，若要使因特网用户能够访问局域网内的服务器，需要设置虚拟服务器条目。

"虚拟服务器"定义了路由器的因特网服务端口与局域网服务器 IP 地址之间的对应关系。因特网所有对此端口的服务请求都会转发给通过 IP 地址指定的局域网服务器，这样既保证了因特网用户成功访问局域网中的服务器，又不影响局域网内部的网络安全。

选择菜单**转发规则→虚拟服务器**，可以在图 5-24所示界面中查看和编辑虚拟服务器条目。



图 5-24 虚拟服务器

点击**添加新条目**按钮，可以在图 5-25所示界面中设置新的虚拟服务器条目。

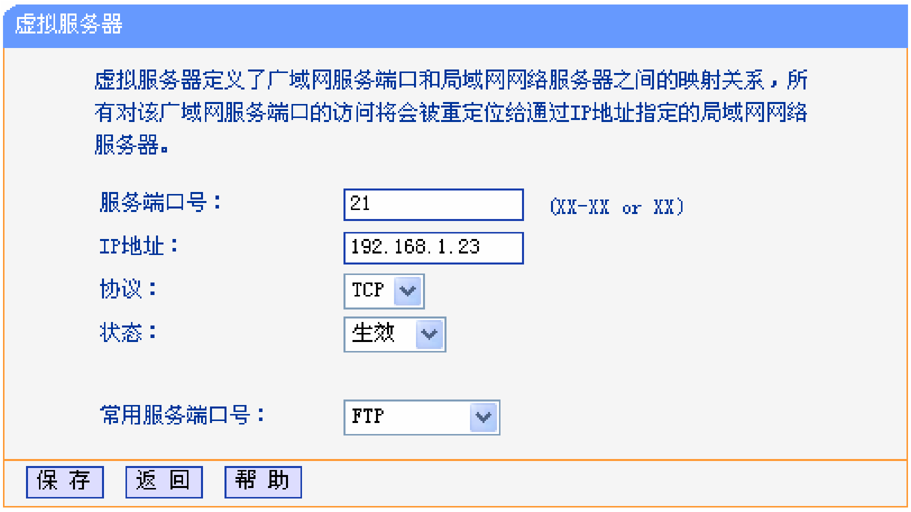


图 5-25 设置虚拟服务器条目

服务端口号： 设置路由器向因特网开放的服务端口。因特网用户通过向该端口发送请求来获取服务。可输入单个端口值或连续的端口段。端口段输入格式为"开始端口-结束端口"。

IP 地址： 输入局域网服务器的静态 IP 地址。通过此 IP 地址，路由器会将对服务端口的访问请求转到局域网服务器上。

协议： 选择此虚拟服务所采用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。

状态： 设置该条目是否生效。只有状态为生效时，本条目的设置才有效。

常用服务端口号： 选择服务器提供的服务类型，系统会自动将该服务的服务端口号和协议添加到上述对应项中。对于"常用服务端口号"中没有列出的服务，需要手动输入服务端口号和协议的相关信息。

举例：假如您有一些大型文件要共享给局域网以外的朋友，而由于文件太大，传输起来不方便，这时可以将自己的计算机构建成 FTP 服务器，然后利用本路由器的虚拟服务器功能使您的朋友可以访问您计算机中的这些文件。假设 FTP 服务器（即您的计算机）的静态 IP 地址为 192.168.1.23，您希望朋友能够通过默认端口 21 访问此服务器，且采用 TCP 协议，那么，请按如下步骤进行设置：

1. 在图 5-24所示的"虚拟服务器"页面点击**添加新条目**按钮。
2. 按图 5-25所示进行设置。其中的服务端口号和协议，可以手动输入，也可以通过在"常用服务端口号"中选择"FTP"，使其对应的端口号"21"和协议"TCP"自动填入到相应设置框中。
3. 单击**保存**按钮，可以看到设置完成后的虚拟服务列表如图 5-24所示。

当您的朋友访问此 FTP 服务器时，只需在浏览器中输入 ftp://xxx.xxx.xxx.xxx:21 即可。其中，"xxx.xxx.xxx.xxx"是本路由器的 WAN 口 IP 地址，如：当路由器 WAN 口 IP 为 172.32.90.1 时，需在浏览器中输入 ftp://172.32.90.1:21。

☞ **注意：**

如果设置了服务端口为80的虚拟服务器，则需要将**安全设置→远端WEB管理**的"WEB管理端口"设置为80以外的值，如88，否则会与路由器远程服务端口发生冲突，因特网用户对此端口的访问将默认为对路由器的访问，而不会转到局域网服务器上，从而导致虚拟服务器不起作用。

5.8.2 特殊应用程序

特殊应用程序功能，可以使某些需要多条连接的应用程序，如 Internet 网络游戏、视频会议、网络电话等能够与网络服务器建立正常连接。

对于此类特殊的应用程序，在客户端向因特网服务器主动发起连接的同时，也需要服务器向客户端发起连接。但在缺省情况下，因特网服务器向局域网客户端发起的连接请求都会被路由器拒绝，导致连接中断。

通过设置**特殊应用程序**，当局域网中有此类请求时，应用程序向触发端口发起连接，会触发路由器打开所有开放端口来为正常连接提供保证。

选择菜单**转发规则→特殊应用程序**，可以在图 5-26所示界面中查看和编辑特殊应用程序条目。



图 5-26 特殊应用程序

点击**添加新条目**按钮，可以在下图 5-27所示界面中设置新的特殊应用程序条目。



图 5-27 设置特殊应用程序条目

触发端口： 该端口是应用程序首先发起连接的端口，只有在该端口上发起连接，开放端口中的所有端口才可以开放。

触发协议： 触发端口上使用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。

开放端口： 当应用程序向触发端口上成功发起连接后，触发对应的开放端口，因特网服务器可通过开放端口与内网计算机连接。可输入单个端口值或端口段。端口段输入格式为“开始端口-结束端口”，不同的端口段用“,”隔开。

开放协议： 开放端口上使用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。

状态： 设置该条目是否生效。只有状态为生效时，本条目的设置才有效。

常用应用程序： 选择需要设置的应用程序，系统会自动将该应用程序的触发端口号和开放端口号添加到上述对应项中。对于"常用应用程序"中没有列出的程序，需要手动输入触发端口和开放端口的相关信息。

5.8.3 DMZ主机

局域网中设置 DMZ（Demilitarized Zone，非军事区）主机后，该主机将完全暴露给广域网，可以实现双向无限制通信。

DMZ 主机实际上就是一个开放了所有端口的虚拟服务器，当需要设置的虚拟服务器的开放端口不确定时，可以把它设置成 DMZ 主机。

选择菜单**转发规则→DMZ主机**，可以在图 5-28所示界面中设置DMZ主机。

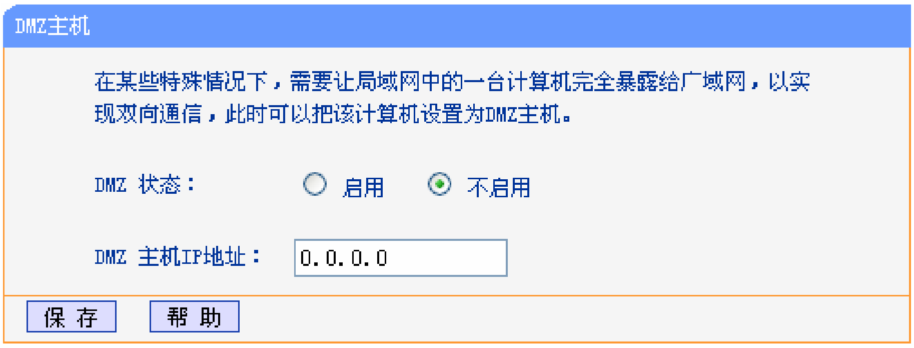


图 5-28 DMZ 主机

DMZ 状态： 选择是否启用 DMZ 主机功能。

DMZ 主机 IP 地址： 输入要设置为 DMZ 主机的局域网计算机的静态 IP 地址。

完成设置后，点击**保存**按钮。

因特网用户访问DMZ主机的方法与访问虚拟服务器的方法一样，具体可参考5.8.1 虚拟服务器的"举例"部分。

☞ 注意：

1. 添加DMZ主机可能会给该主机带来不安全因素，因此不要轻易使用这一选项。
2. DMZ主机的优先级低于虚拟服务器，因特网用户对路由器同一端口的访问将优先转发到虚拟服务器所对应的局域网服务器上。

5.8.4 UPnP设置

依靠 UPnP(Universal Plug and Play，通用即插即用)协议功能，局域网中的主机可以请求路由器自动进行端口转换，使得外部主机能够在需要时访问内部主机上的资源，如 Windows XP 和 Windows ME 系统上安装的 MSN Messenger 或迅雷、BT、PPLive 等支持 UPnP 协议的应用程序。

选择菜单**转发规则→UPnP设置**，可以在图 5-29所示界面中查看UPnP信息。

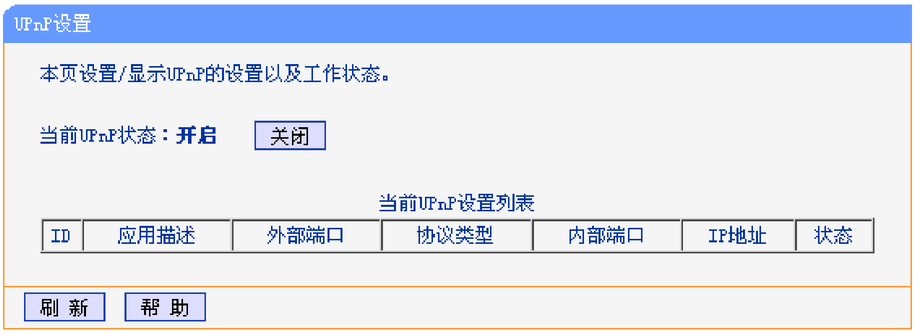


图 5-29 UPnP 设置

应用描述： 显示应用程序通过 UPnP 向路由器请求端口转换时给出的描述。

外部端口： 显示端口转换时使用的路由器端口号。

协议类型： 显示进行端口转换时采用的协议类型。

内部端口： 显示需要进行端口转换的局域网主机端口号。

IP 地址： 显示需要进行端口转换的局域网主机 IP 地址。

状态： 显示该条目是否已经启用。

使用时点击**开启**按钮即可，端口转换信息由应用程序发出请求时提供，无需进行任何设置。点击**刷新**按钮可以看到当前正在使用本功能的应用程序的端口转换相关信息，如图 5-29。

☞ 注意：

1. 因为现阶段版本的UPnP协议的安全性还未得充分保证，不使用时请关闭UPnP功能。
2. 只有支持UPnP协议的应用程序才能使用本功能。
3. UPnP功能需要操作系统的支持(如Windows ME/Windows XP/Windows Vista)。

5.9 安全设置

选择菜单**安全设置**，您可以看到：



单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.9.1 防火墙设置

选择菜单**安全设置→防火墙设置**，您可以在下图 5-30界面中设置路由器的安全项。

该界面控制路由器防火墙总功能的开启，以及各子项功能：IP地址过滤、域名过滤和MAC地址过滤功能的开启和过滤规则。只有防火墙的总开关开启后，后续的安全设置才能够生效，反之，则不能生效。(建议在过滤规则设置完成后再开启防火墙总开关)



图 5-30 防火墙设置

开启防火墙： 这是防火墙的总开关，只有该项开启后，IP地址过滤、域名过滤、MAC地址过滤功能才能启用，反之，则不能被启用。

开启IP地址过滤： 关闭或开启IP地址过滤功能并选择缺省过滤规则。只有“开启防火墙”启用后，该项才能生效。

开启域名过滤： 关闭或开启域名过滤功能。只有“开启防火墙”启用后，该项才能生效。

开启MAC地址过滤： 关闭或开启MAC地址过滤功能并选择缺省过滤规则。只有“开启防火墙”启用后，该项才能生效。

完成设置后，点击**保存**按钮。

5.9.2 IP地址过滤

选择菜单**安全设置→IP地址过滤**，您可以在下图 5-31界面中查看并添加IP地址过滤条目。

使用IP地址过滤可以拒绝或允许局域网中计算机与互联网之间的通信。可以拒绝或允许特定IP地址的特定的端口号或所有端口号。

您可以利用按钮**添加新条目**来增加新的过滤规则，或者通过“修改”、“删除”链接来修改或删除已设过滤规则，甚至可以通过按钮**移动**来调整各条过滤规则的顺序，以达到不同的过滤优先级(ID序号越靠前则优先级越高)。



图 5-31 IP 地址过滤

生效时间： 该项用来指定过滤条目的有效时间，在该段时间外，此过滤条目不起作用。

局域网IP地址： 局域网中被控制的计算机的IP地址，为空表示对局域网中所有计算机进行控制。此处可以输入一个IP地址段，例如：192.168.1.123－192.168.1.185。

(局域网)端口： 局域网中被控制的计算机的服务端口，为空表示对该计算机的所有服务端口进行控制。此处可以输入一个端口段，例如：1030－2000。

广域网IP地址： 广域网中被控制的计算机(如网站服务器)的IP地址，为空表示对整个广域网进行控制。此处可以输入一个IP地址段，例如：61.145.238.6-61.145.238.47。

(广域网)端口： 广域网中被控制的计算机(如网站服务器)的服务端口，为空表示对该网站所有服务端口进行控制。此处可以输入一个端口段，例如：25-110。

协议： 此处显示被控制的数据包所使用的协议。

通过： 该项显示符合本条目所设置的规则的数据包是否可以通过路由器，“是”表示允许该条目通过路由器，“否”表示不允许该条目通过路由器。

状态： 显示该条目状态“生效”或“失效”，只有状态为生效时，本条过滤规则才生效。

举例：如果您希望禁止局域网中IP地址为192.168.1.7的计算机在8：30到18：00之间收发邮件，禁止IP地址为192.168.1.8的计算机在8：00到18：00之间访问IP为202.96.134.12的网站，对局域网中的其它计算机则不做任何限制，这时您可以按照如下步骤设置：

1. 在图 5-30界面中打开防火墙总开关。
2. 在图 5-30中开启“IP地址过滤”，设置“缺省过滤规则”为“凡是不符合已设IP地址过滤规则的数据包，允许通过本路由器”。
3. 在图 5-31界面中点击**添加新条目**，然后在下图 5-32中按要求添加过滤条目。下图是禁止 192.168.1.7 的计算机在 8：30 到 18：00 之间发送邮件的设置，设置完成后点击**保存**按钮。



图 5-32 添加 IP 地址过滤条目

4. 回到第 3 步，继续设置过滤条目：禁止局域网中 IP 地址为 192.168.1.7 的计算机在 8：30 到 18：00 之间接收邮件，禁止 IP 地址为 192.168.1.8 的计算机在 8：00 到 18：00 之间访问 IP 为 202.96.134.12 的网站。完成例 1 中设置一共需要设置 3 条 IP 过滤规则，依次对应下面列表中的三条过滤条目。

ID	生效时间	局域网IP地址	端口	广域网IP地址	端口	协议	通过	状态	配置
1	0830-1800	192.168.1.7	-	-	25	ALL	否	生效	编辑 删除
2	0830-1800	192.168.1.7	-	-	110	ALL	否	生效	编辑 删除
3	0800-1800	192.168.1.8	-	202.96.134.12	-	ALL	否	生效	编辑 删除

5.9.3 域名过滤

选择菜单**安全设置→域名过滤**，您可以在下图 5-33界面中查看并添加域名过滤条目。

域名过滤可以阻止LAN中所有计算机访问广域网(如互联网)上的特定域名，该特性会拒绝所有到特定域名如http和ftp的请求。您可以利用按钮**添加新条目**来增加新的过滤规则，或者通过"修改"、"删除"链接来修改或删除旧的过滤规则。



图 5-33 域名过滤

域名： 拒绝被LAN计算机访问的域名。

状态： 显示该条目状态“生效”或“失效”，只有状态为生效时，本条过滤规则才生效。

举例： 如果您希望禁止局域网中的计算机在8：30到18：00之间访问“www.yahoo.com.cn”、“sina.com”的网站，禁止局域网中的计算机在8：00到12：00之间访问所有以“.net”结尾的网站，这时您可以按照如下步骤设置：

1. 图 5-30界面中打开防火墙总开关并开启“域名过滤”。
2. 在图 5-33界面中点击**添加新条目**，然后在下图 5-34界面中设置条目信息。下图是在 8：30 到 18：00 之间拒绝访问www.yahoo.com.cn网站的设置，设置完成后，点击保存按钮。

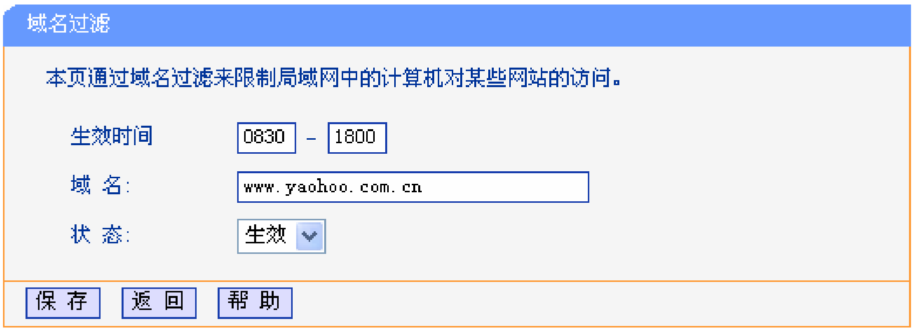


图 5-34 添加域名过滤条目

3. 回到第 2 步，继续设置过滤条目：禁止局域网中的计算机在 8：30 到 18：00 之间访问“sina.com”，禁止局域网中的计算机在 8：00 到 12：00 之间访问所有以“.net”结尾的网站。完成例 1 中设置一共需要设置 3 条域名过滤规则，依次对应下面列表中的三条过滤条目。

ID	生效时间	域 名	状 态	配 置
1	0830-1800	www.yaohoo.com.cn	生效	编辑 删除
2	0830-1800	sina.com	生效	编辑 删除
3	0800-1200	.net	生效	编辑 删除

5.9.4 MAC地址过滤

选择菜单**安全设置→MAC地址过滤**，您可以在下图 5-35界面中查看并添加MAC地址过滤条目。

MAC地址过滤功能通过MAC地址允许或拒绝局域网中计算机访问广域网，有效控制局域网内用户的上网权限。您可以利用按钮**添加新条目**来增加新的过滤规则；或者通过“修改”、“删除”链接来修改或删除旧的过滤规则。



图 5-35 MAC 地址过滤

MAC地址： 该项是您希望管理的计算机的MAC地址。

描述： 该项是对该计算机的适当描述。

状态： 显示该条目状态“生效”或“失效”，只有状态为生效时，本条过滤规则才生效。

举例：如果您不希望局域网中MAC地址为00-E0-4C-00-07-BE和00-E0-4C-00-07-5E的计算机访问Internet，而希望局域网中的其它计算机能访问Internet，这时您可以按照如下步骤设置MAC地址过滤表：

1. 在图 5-30界面中打开防火墙总开关。
2. 在图 5-30防火墙设置界面中开启“MAC地址过滤”，设置“缺省过滤规则”为“禁止已设MAC地址列表中已启用的MAC地址访问Internet，允许其它MAC地址访问Internet”。
3. 在图 5-35界面中点击**添加新条目**，然后在下图 5-36界面中设置条目信息。下图是禁止MAC地址为 00-E0-4C-00-07-BE的计算机访问Internet的设置，设置完成后，点击**保存**按钮。

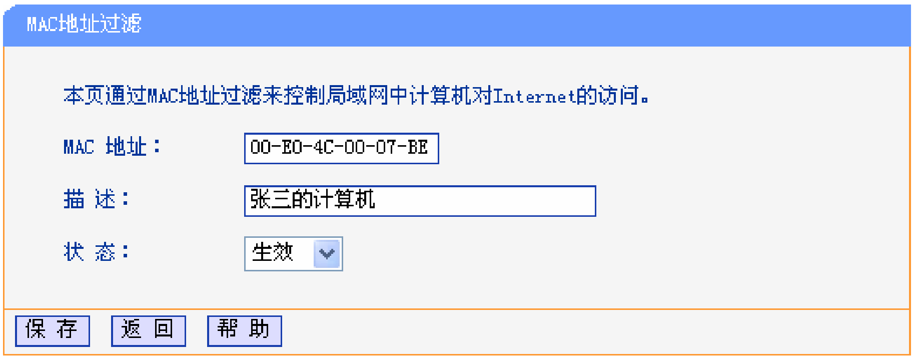


图 5-36 添加 MAC 地址过滤条目

4. 回到第 3 步，继续设置过滤条目：禁止 MAC 地址为 00-E0-4C-00-07-5E 的计算机访问Internet。完成例 1 中设置一共需要设置 2 条域名过滤规则，依次对应如下列表中的 2 条过滤条目。

ID	MAC地址	描 述	状 态	配 置
1	00-E0-4C-00-07-BE	张三的计算机	生效	编辑 删除
2	00-E0-4C-00-07-5E	李四的计算机	生效	编辑 删除

5.9.5 远端WEB管理

选择菜单**安全设置→远端WEB管理**。远端WEB管理功能可以允许用户通过Web浏览器从广域网配置路由器。本特性允许您从远程主机执行管理任务。您可以在下图 5-37界面中设置管理IP地址和端口。

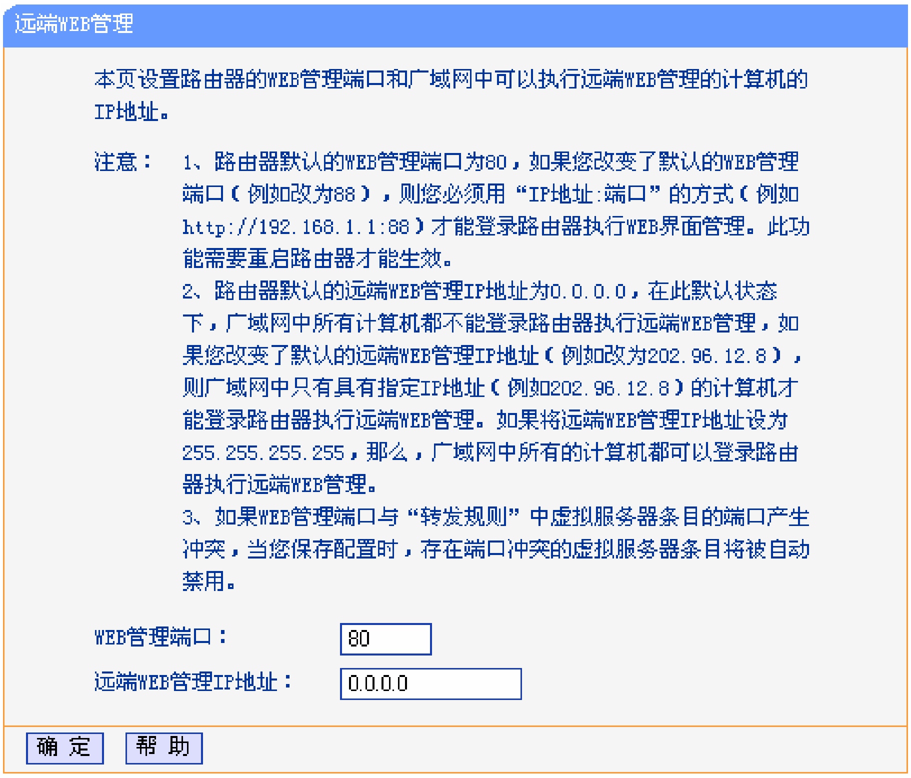


图 5-37 远端 WEB 管理

WEB管理端口： 用于访问宽带路由器的WEB管理端口号。

远端WEB管理IP地址： 广域网中可以访问该路由器执行远端WEB管理的计算机IP地址。

完成更改后，点击**保存**按钮。

☞ 注意：

1. 路由器默认的WEB管理端口为80，如果您改变了默认的WEB管理端口(例如改为88)，则您必须用“IP地址:端口”的方式(例如http://192.168.1.1:88)才能登录路由器执行WEB界面管理。此功能需要重启路由器后才生效。
2. 路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果您改变了默认的远端WEB管理IP地址(则广域网中只有具有该指定IP地址的计算机才能登录路由器执行远端WEB管理。如果改为255.255.255.255，则WAN中所有主机都可以登录路由器执行远端WEB管理。

举例：如果您希望广域网中IP地址为202.96.134.13的计算机能够访问宽带路由器，执行远端WEB管理功能，WEB管理端口为80。则您可以进行如下设置：

1. 设置 WEB 管理端口为“80”。
2. 设置远端 WEB 管理 IP 地址为“255.255.255.255”或“202.96.134.13”。

这样，该计算机访问路由器管理界面时应该输入路由器WAN口IP地址即可。

5.9.6 高级安全设置

选择菜单**安全设置→高级安全设置**，您可以在下图 5-38界面中开启DoS(拒绝服务)攻击防范。完成更改后，点击**保存**按钮。

DoS攻击的目的是用极大量的虚拟信息流耗尽目标主机的资源，受害者被迫全力处理虚假信息流，从而影响对正常信息流的处理。如果DoS攻击始发自多个源地址，则称为分布式拒绝服务(DDoS)攻击。通常DoS与DDoS攻击中的源地址都是欺骗性的。

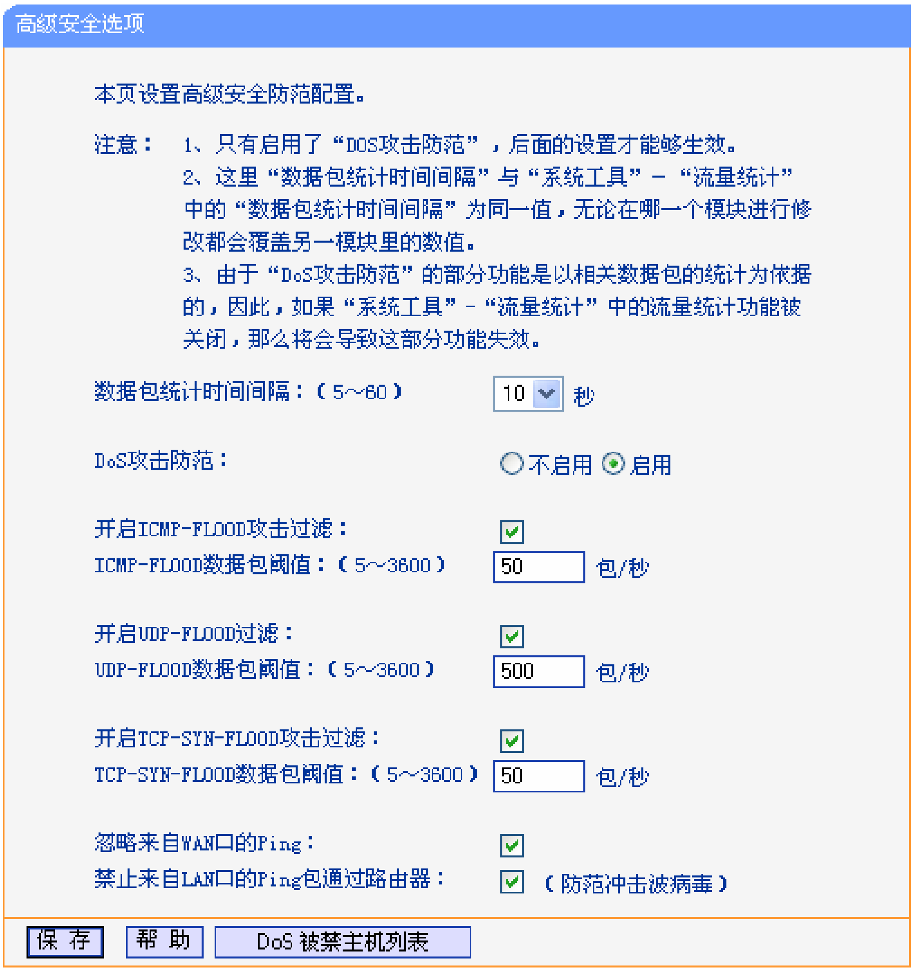


图 5-38 WAN 口 Ping

数据包统计时间间隔：

该项设置对ICMP、UDP、TCP数据包进行统计的时间间隔，即在当前时间间隔内对各种数据包进行统计，如果统计得到的某种数据包(例如UDP FLOOD)达到了指定的阈值，那么系统将认为UDP-FLOOD 攻击已经发生，如果UDP-FLOOD过滤已经开启，那么路由器将会停止接收该类型的数据包,从而达到防范攻击的目的。

DoS攻击防范： 该项是开启下面各种攻击防范的总开关，只有选择此项后，以下的几种防范措施才能生效。

开启ICMP-FLOOD攻击过滤：

若需要防范ICMP-FLOOD攻击，请选择此项。

ICMP-FLOOD数据包阈值：

当开启ICMP-FLOOD功能后，如果在指定时间间隔内ICMP包达到了指定的数目，防范措施则立即启动。

开启**UDP-FLOOD**攻击过滤：

若需要防范UDP-FLOOD，请选择此项。

UDP-FLOOD数据包阈值：

当开启UDP-FLOOD功能后，如果在指定时间间隔内UDP包达到了指定的数目，防范措施则立即启动。

开启**TCP-SYN-FLOOD**攻击过滤：

若需要防范TCP-SYN-FLOOD，请选择此项。

TCP-SYN-FLOOD数据包阈值：

当开启TCP-SYN-FLOOD功能后，如果在指定时间间隔内TCP的SYN包达到了指定的数目，防范措施则立即启动。

忽略来自**WAN**口的**Ping：**

若开启该功能，广域网的计算机将不能Ping通路由器。

禁止来自**LAN**口的**Ping**包通过路由器**：**

若开启该功能，局域网的计算机将不能Ping通广域网中的计算机。

DoS被禁主机列表：

点击该按钮，你可以查看被禁止的主机列表，如图 5-39。单击**刷新**按钮可以更新列表信息。若希望被禁主机能够重新上网，可以点击**删除**按钮；若需要释放所有被禁主机，可以点击**清空**按钮。

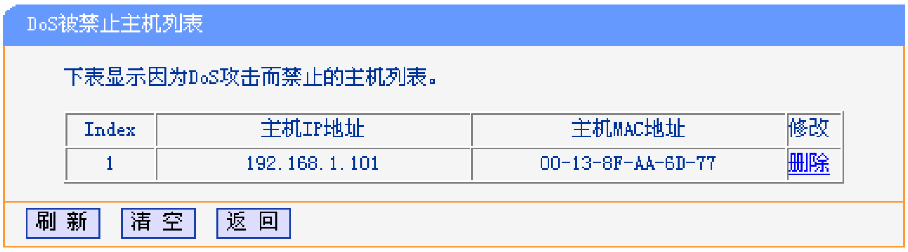


图 5-39 DoS 被禁主机列表

5.10 路由功能

选择菜单**路由功能**，可以看到：



单击**静态路由表**，即可进行静态路由功能设置，下面将详细讲解静态路由功能的设置。

5.10.1 静态路由表

静态路由是一种特殊的路由，由网络管理员手动配置。在网络中使用合适的静态路由可以减少路由选路造成的网络开销，提高数据包的转发速度。

静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

通过设定目的 IP 地址、子网掩码和网关地址可以确定一个路由条目。其中目的 IP 地址和子网掩码用来确定一个目标网络/主机，然后路由器会将数据包发往相应静态路由条目的网关，并由该网关转发数据包。

☞ 注意：

当路由器周围的网络环境较复杂，或者没有完全了解周围网络的拓扑结构时，请慎用此功能。

选择菜单**路由功能→静态路由表**，可以在下图 5-40的界面中设置静态路由信息。



图 5-40 静态路由表

点击**添加新条目**按钮，你可以在下图中添加静态路由条目。如图 5-41。



图 5-41 添加静态路由条目

目的 IP 地址： 用来标识希望访问的目标地址或目标网络，此 IP 地址不能和路由器的 WAN 口或 LAN 口 IP 地址处于同一网段。

子网掩码： 该项与目的 IP 地址一起来标识目标网络。

默认网关： 数据包被指定发往的下一个节点的 IP 地址，此 IP 地址必须和路由器的 WAN 口或 LAN 口 IP 地址处于同一网段。

状态： 显示该条目是否生效。只有状态为生效时，此路由条目才起作用。

5.11 IP带宽控制

带宽控制功能可以实现对局域网计算机上网带宽的控制。在带宽资源不足的情况下，通过对各类数据包的带宽进行控制，可以实现带宽的合理分配，达到有效利用现有带宽的目的。通过 IP 带宽控制功能，可以设置局域网内主机的带宽上下限，保证每台主机都能通畅地共享网络，并在网络空闲时充分利用网络带宽。

选择菜单**IP带宽控制**，将进入下图 5-42所示界面。在此界面中，您可以开启或关闭IP带宽控制功能，并设置IP带宽控制规则。



图 5-42 IP 带宽控制设置功能设置

开启IP带宽控制：

选择是否开启IP带宽控制功能，只有此处开启时，后续的“控制规则”设置才能够生效。

带宽线路类型：您申请的带宽线路类型，此处仅区分ADSL线路和其它线路。

申请的带宽大小：

您申请的带宽大小，如果此处填写的值与实际不符，IP带宽控制功能可能会受影响。

以下为IP带宽控制规则列表中的各项说明：

IP地址段：受该条规则限制的IP地址（或IP地址段），不同规则的IP地址不能有交集。

模式：对该条规则中的IP地址（或IP地址段）进行限制的方式。

带宽大小：如果该条规则的模式为“保障最小带宽”，受该条规则限制的IP地址（或IP地址段）的带宽总和至少可以达到此值；如果该条规则的模式为“限制最大带宽”，受该条规则限制的IP地址（或IP地址段）的带宽总和最多只能达到此值。

备注：对该条规则的文字说明，不超过10个字（包括标点符号）。

启用：是否启用该条规则。

完成设置后，点击**保存**按钮。

5.12 IP与MAC绑定

IP 与 MAC 绑定，可以有效防止 ARP 攻击，维护局域网用户的上网安全。

选择菜单 **IP 与 MAC 绑定菜单**，可以看到：



单击菜单中的子项即可进行具体的设置，下面将详细讲解两个子项的功能和设置方法。

5.12.1 静态ARP绑定设置

静态 ARP 绑定，即 IP 与 MAC 绑定，是防止 ARP 攻击本路由器的有效方法。

路由器在局域网内传输 IP 数据包时是靠 MAC 地址来识别目标的，因此 IP 地址与 MAC 地址必须一一对应，这些对应关系靠 ARP 映射表来维护。ARP 攻击可以用伪造的信息更新路由器的 ARP 映射表，破坏表中 IP 地址与 MAC 地址的对应关系，使路由器无法与相应的主机进行通信。

静态 ARP 绑定将主机的 IP 地址与相应的 MAC 地址进行绑定，可以有效防止 ARP 列表被错误的 IP MAC 对应信息更替。

选择菜单**IP与MAC绑定→静态ARP绑定设置**，可以在图 5-43所示界面中设置静态ARP绑定条目。



图 5-43 静态 ARP 绑定设置

ARP绑定： 选择是否开启ARP绑定功能，只有选择"启用"并单击**保存**后，列表中的设置才能生效。

点击**增加单个条目**按钮，可以在图 5-44所示界面中设置新的静态ARP绑定条目。

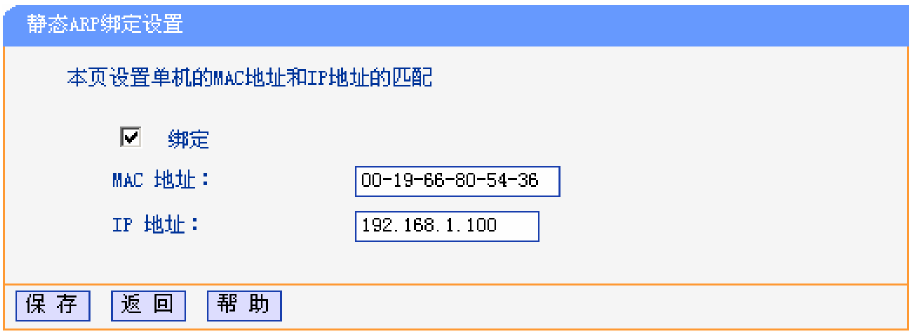


图 5-44 添加静态 ARP 绑定条目

绑定： 设置本条目状态，只有选中该项，该条绑定条目才能生效。

MAC 地址： 输入被绑定主机的 MAC 地址。

IP 地址： 输入被绑定主机的 IP 地址。

5.12.2 ARP映射表

如前所述，IP 数据包在局域网内传输时是靠 MAC 地址来识别目标的，IP 地址与 MAC 地址必须一一对应，ARP 映射表就是用来存储与维护这些对应信息的。

选择菜单**IP与MAC绑定→ARP映射表**，可以在图 5-45所示界面中查看ARP条目信息。



ARP映射表

ID	MAC地址	IP地址	状态	配置
1	00-0F-E2-80-30-90	172.31.70.1	未绑定	导入 删除
2	00-19-66-80-54-37	172.31.70.88	未绑定	导入 删除
3	00-19-66-80-54-36	192.168.1.100	未绑定	导入 删除

全部绑定 全部导入 刷 新 帮 助

图 5-45 ARP 映射表

导入： 将相应条目的ARP信息添加到图 5-43界面的静态ARP绑定列表中。

全部导入： 将当前ARP映射列表中所有条目的信息添加到图 5-43界面的静态ARP绑定列表中。

全部绑定： 将当前 ARP 映射列表中所有条目的状态设置为绑定，注意该按钮只有在启用了 ARP 绑定功能后才能点击。

☞ **注意：**

1. 在进行导入操作时，如果该条目与ARP静态绑定表中的某条目有冲突，则会显示冲突提示，而且不会导入该条目。
2. 在进行全部导入操作时，如果同样存在冲突条目，则系统会忽略冲突条目，将其它没有冲突的条目添加到ARP静态绑定列表中。

举例：假如局域网内计算机的静态 IP 地址为 192.168.1.100，MAC 地址为 00-19-66-80-54-36，为防止 ARP 攻击影响计算机的正常通信，请通过以下方法进行 ARP 绑定操作：

方法一：

1. 在图 5-43所示界面中启用ARP绑定并单击**保存**按钮。
2. 点击**增加单个条目**按钮。
3. 按图 5-44所示进行设置。
4. 单击**保存**按钮，可以看到设置完成后的ARP绑定条目如图 5-43所示。

方法二：

1. 在图 5-45所示界面中找到IP地址 192.168.1.100 和MAC地址 00-19-66-80-54-36 对应的条目，单击相应的**导入**按钮。
2. 返回图 5-43所示界面，在列表中选中导入条目对应的“绑定”。
3. 启用 ARP 绑定并单击**保存**按钮。

提示：

此处的ARP绑定只是在路由器上绑定了主机的IP MAC地址，因此只能使路由器免受ARP攻击。为保证上网安全，您还需在自己的计算机上绑定路由器LAN口的IP MAC地址，建议使用ARP防火墙来实现此功能。

5.13 动态DNS

动态DNS又名DDNS，它的主要功能是实现固定域名到动态IP地址之间的解析。如果路由器的WAN口IP地址为动态获取的，通过此功能可使互联网上的其它主机用固定域名的方式访问路由器或虚拟服务器。

动态DNS功能对于使用动态IP地址的用户，在每次上网得到新的IP地址后，路由器内置的动态域名软件就会将该IP地址发送到由DDNS服务商提供的动态域名解析服务器，并更新域名解析数据库。当Internet上的其他用户需要访问这个域名的时候，动态域名解析服务器就会返回正确的IP地址。此功能对于大多数不使用固定IP地址的用户，也可以经济、高效地构建自身的服务网络。

选择菜单**动态DNS**，你可以在图 5-46中设置动态DNS功能。只需在花生壳官方网站上进行注册，以相应的用户名/密码登录并启用DDNS功能即可。



图 5-46 动态 DNS 设置

服务商链接： 如果你还未在DDNS上注册，请选择“花生壳动态域名解析服务申请”进行注册。

服务提供者： 选择提供DDNS的服务器，本路由器内置花生壳DDNS客户端。单击“注册”可以登录花生壳首页进行注册。

用户名、密码： 请正确填写在DDNS上注册的用户名和密码。

启用DDNS： 该项用来启用花生壳DDNS服务。

登录/退出： 点击该按钮，可以登录/退出DDNS服务。

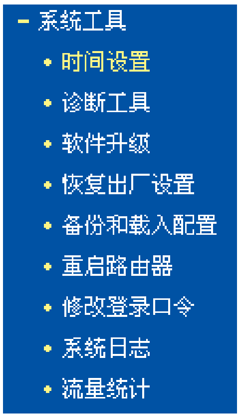
图 5-46为注册成功后，用注册的Oray护照和密码登录到DDNS服务器上的连接成功示意图。当连接状态显示成功后，互联网上的其它主机就可以通过域名信息中的域名来访问路由器或虚拟服务器。

提示：

若希望将局域网中的服务器向互联网开放，则还需要在转发规则功能中设置相应的端口映射，具体设置请参考5.8 转发规则部分。

5.14 系统工具

在系统工具中，可以对路由器进行优化配置。



- 时间设置，用于设置当地所在时区，获取准确的网络时间。
- 诊断工具，用来检测路由器与其他网络设备的连接状况。
- 软件升级，用于通过 Web 页面升级路由器的软件版本。
- 恢复出厂设置，用于恢复路由器的出厂默认设置。
- 备份和载入配置，用于备份系统设置信息，并在需要时将其重新载入。
- 重启路由器，用于通过 Web 页面重新启动路由器。
- 修改登录口令，用于修改登录本 Web 页面的用户名和密码，防止非授权人员随意登录 Web 设置页面。
- 系统日志，用于查看系统日志信息以快速定位设备故障或了解网络情况。
- 流量统计，用于实时查看局域网用户通过路由器进行通信的情况。

单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.14.1 时间设置

选择菜单**系统工具→时间设置**，可以在下图 5-47界面中设置路由器的系统时间。设置系统时间有两种方式，手动设置系统时间和通过互联网获取标准的GMT时间。

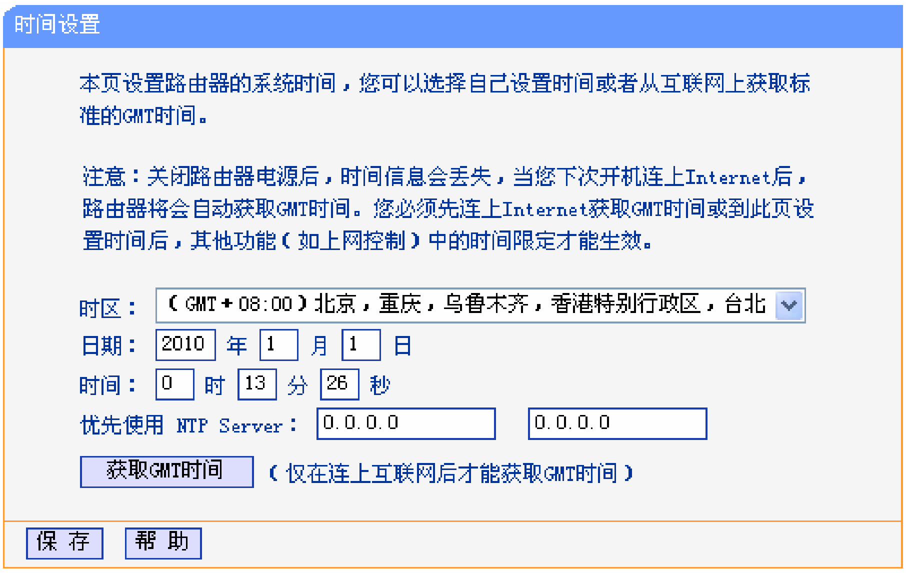


图 5-47 时间设置

优先使用NTP Server： 该项用来设置NTP Server的IP地址(最多可以输入两个)。NTP Server是网络时间服务器，用于同步互联网上的计算机时间。该路由器中内置了一些常用的NTP Server地址，一旦与Internet连接后，路由器可以自动获取系

统时间。但是，若此处设置了该项，则当路由器获取GMT时间时，将优先从已设置的时间服务器上获取。

时间设置方式：

手动设置时间： 首先请选择所在的时区，然后在日期和时间栏内填入相应值，最后单击**保存**按钮即可完成系统时间的设置。

获取GMT时间： 首先请连接互联网，然后选择所在的时区，最后单击**获取GMT时间**按钮即可从互联网上获取标准的GMT时间。

☞ 注意：

1. NTP（Network Time Protocol, 网络时间协议）用来为路由器、交换机和工作站之间提供时间同步。时间同步的作用是可以将多台网络设备上的相关事件记录联系起来，有助于分析复杂的故障和安全事件等。
2. 关闭路由器电源后，时间信息会丢失，只有当下次开机连上Internet后，路由器才会自动获取GMT时间。
3. 必须先通过Internet获取GMT时间或在此页手动设置系统时间后，路由器其他功能(如防火墙)中的时间限定才能生效。

5.14.2 诊断工具

选择菜单**系统工具→诊断工具**，可以在下图 5-48界面中通过使用Ping或Tracert功能来测试路由器和其它主机（包括网络设备）的连接情况。



图 5-48 诊断工具

选择操作： 选择使用Ping或Tracert功能来检测路由器的连接状态。其中Ping功能用来检测路由器和被测主机是否已连通及连接延时等，而Tracert功能用来检测路由器要连通被测主机时需经过的其他路由器的个数。

IP地址/域名： 与路由器连接的设备的IP地址或域名。

Ping包数目： Ping操作发出的Ping包数目，推荐保持默认值4。

Ping包大小： Ping操作发出的Ping包的大小，推荐保持默认值64。

Ping超时： 设置Ping操作的超时时间。即超过这个时间没收到回应（Reply）时，认为Ping操作失败。

Tracert跳数： 设置Tracert的跳数，即超过此跳数值还没有连通待测设备时，将被判定为连接失败。

填好相关参数后单击**开始**按钮，路由器就开始进行相应的Ping或Tracert测试了，并显示测试结果。

下图5-49是路由器与域名为www.baidu.com的主机正常连接时使用Ping功能诊断的结果，图 5-50是路由器与域名为www.baidu.com的主机没有连通时使用Ping功能诊断的结果。



图 5-49 Ping 诊断结果—成功

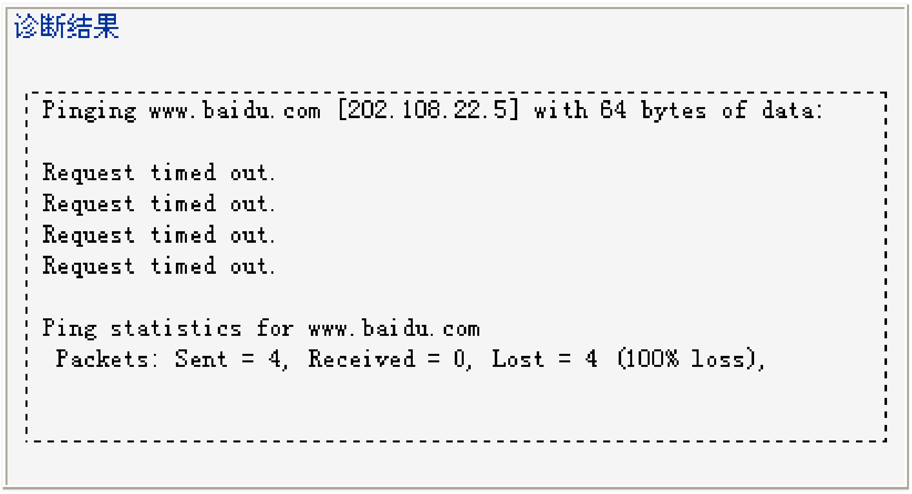


图 5-50 Ping 诊断结果—失败

下图 5-51是路由器与IP地址为 10.145.206.66 的主机正常连接时使用Tracert功能诊断的结果，图 5-52是路由器与IP地址为 10.145.206.66 的主机没有连通时使用Tracert功能诊断的结果。



图 5-51 Tracert 诊断结果—成功

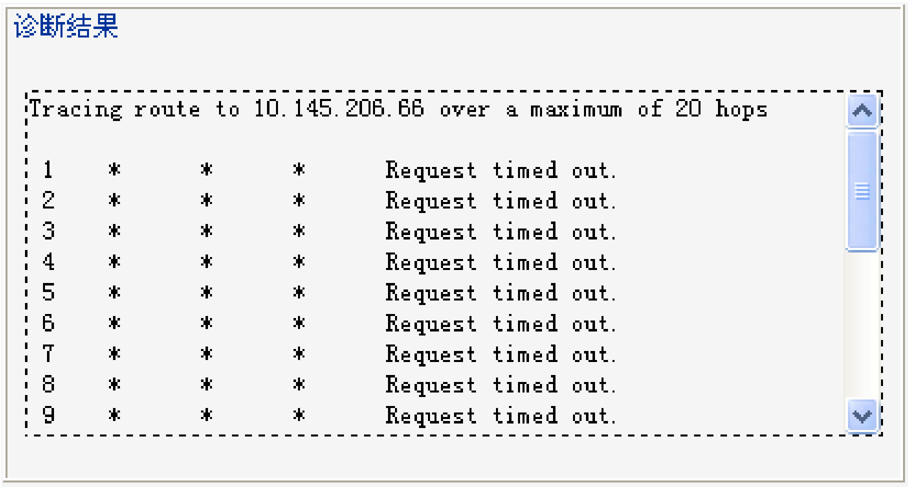


图 5-52 Tracert 诊断结果—失败

5.14.3 软件升级

选择菜单**系统工具→软件升级**，可以在下图 5-53界面中升级本路由器的软件版本以获得更多的功能和更为稳定的性能。



图 5-53 软件升级

软件升级步骤：

第一步：登录本公司的网站(www.tp-link.com.cn)，下载最新版本的软件。

第二步：关闭系统防火墙，包括系统自带的防火墙以及您另外安装的防火墙软件。

第三步：双击打开升级包中的 Tftpd32.exe 文件，并确保在整个升级过程中该软件始终处于开启的状态。

第四步：在图 5-53界面的"文件名"栏内填入已下载升级软件的文件名，如"wr740nv5.bin"。

第五步：单击**升级**进行软件升级。

☞ 注意:

1. 升级软件后，路由器可能会恢复到出厂默认设置，现有的所有设置信息将丢失，建议在升级软件之前备份现有设置信息。
2. 升级时请选择与当前硬件版本一致的软件。升级过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。当升级结束后，路由器将会自动重启。

5.14.4 恢复出厂设置

选择菜单**系统工具→恢复出厂设置**，可以将路由器的所有设置恢复到出厂时的默认状态。恢复出厂设置后，路由器将自动重启，恢复出厂设置页面如图 5-54。

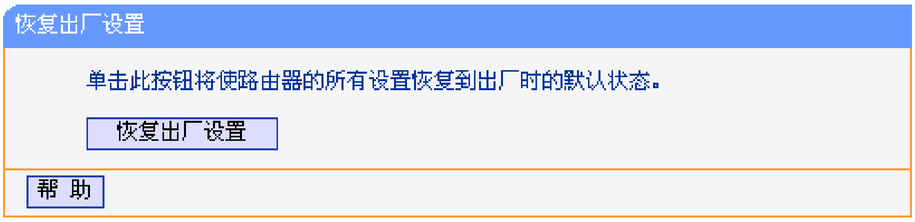


图 5-54 恢复出厂设置

单击**恢复出厂设置**按钮，路由器的所有设置将恢复到出厂时的默认状态。其中：

- 默认的用户名：admin
- 默认的密码：admin
- 默认的IP地址：192.168.1.1
- 默认的子网掩码：255.255.255.0

☞ 注意：

请在恢复出厂设置前备份配置信息。若有需要则可通过载入备份的配置信息来恢复路由器的配置。

5.14.5 备份和载入配置

选择菜单**系统工具→备份和载入配置**，可以在下图 5-55中备份或载入路由器配置文件。

配置备份功能可以将路由器的设置以文件形式保存到电脑中，以备下次使用；在升级路由器软件或在载入新的配置文件前备份路由器的原有配置，可以有效防止升级软件或载入新配置文件过程中丢失原有配置的问题。

配置载入功能则可以将先前保存的或已编辑好的配置文件重新载入。

如果需要为多台路由器配置相同的设置，则可以先配置一台路由器，保存其配置文件后，再将其载入到其它的路由器中，这样可以有效节省配置时间。

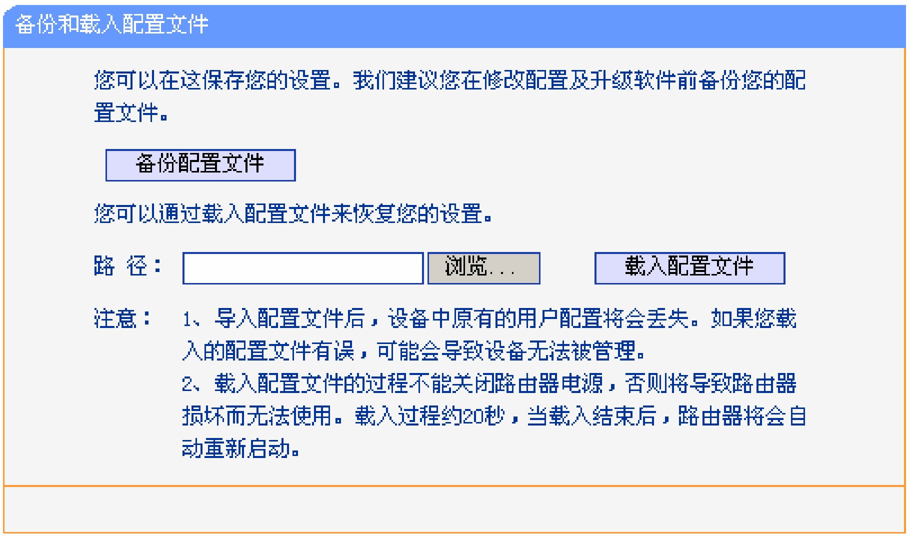


图 5-55 配置文件备份与载入

例1：如果您希望备份现有路由器的配置文件到C:\Router\backup，可以按照如下步骤操作。

1. 在图 5-55界面中点击**备份配置文件**。

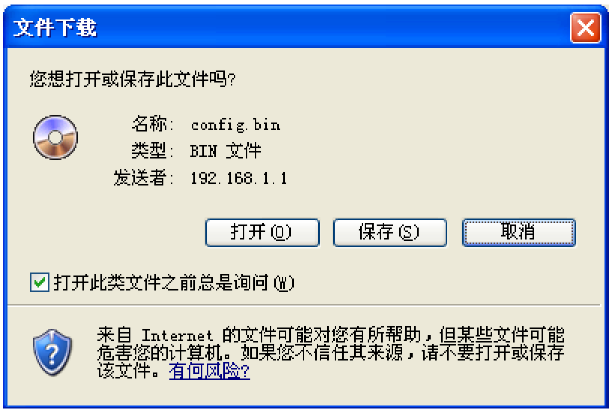


图 5-56 备份配置文件-文件下载

2. 在图 5-56界面中点击**保存**按钮。
3. 在图 5-57界面中选择文件存放路径“C:\Router\backup”，然后点击**保存**按钮即可完成文件备份。

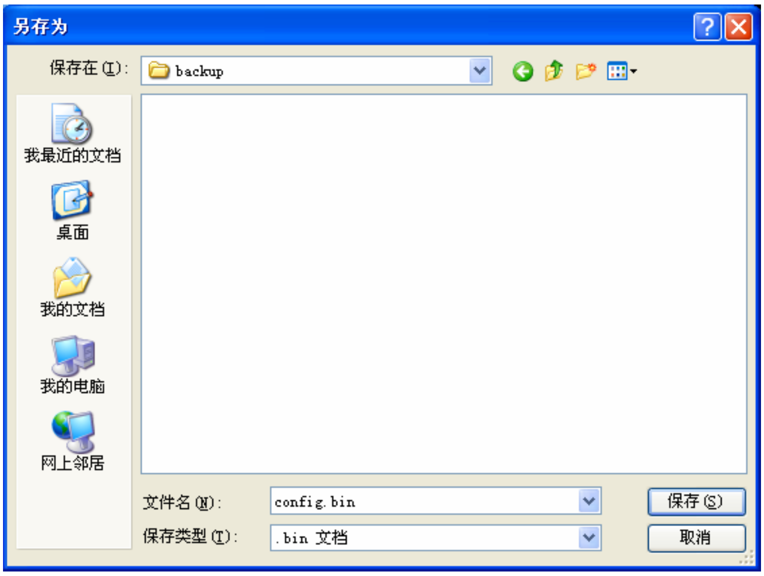


图 5-57 备份配置文件-选择文件存放路径

例2：如果您希望将C:\Router\backup目录下的config.bin文件载入到路由器中，请按照如下步骤操作。

1. 在图 5-55界面中单击**浏览**按钮来选定config.bin文件，或者在“路径”栏中输入文件的全路径“C:\Router\backup\config.bin”。
2. 在图 5-55界面中点击**载入配置文件**按钮即可。

☞ 注意：

1. 载入配置文件后，设备中原有的配置信息将会丢失，所以在导入配置文件前请先备份配置。如果载入的配置文件有误，可重新载入先前备份的文件。
2. 配置文件载入的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重新启动。如果载入有错，请根据提示信息自己选择是否保存配置，最好能重启路由器。

5.14.6 重启路由器

选择菜单**系统工具→重启路由器**，可以将路由器重新启动，如图 5-58。

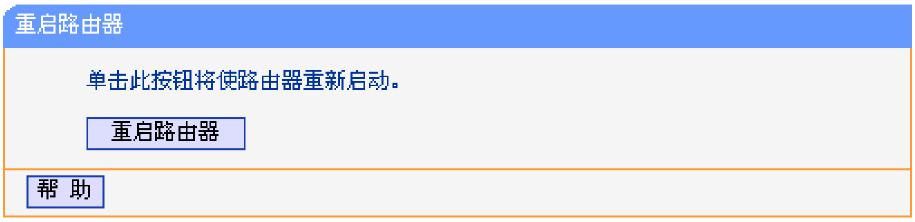


图 5-58 重启路由器

本路由器的某些设置需要在路由器重新启动后才能生效。

- 设置后系统能自动重启的项目有：
  - 对路由器进行软件升级
  - 恢复路由器的出厂设置
  - 修改 LAN 口的基本网络参数
- 设置后需手动重启路由器才能生效的项目有：
  - 设置 QSS 安全设置功能
  - 设置 DHCP 服务功能
  - 设置 DHCP 服务器的静态地址分配功能
  - 设置无线网络的基本参数
  - 修改无线网络的安全设置
  - 修改无线网络的高级设置
  - 修改路由器的远程 WEB 管理端口

手动重启的方法：单击图 5-58中的**重启路由器**按钮。

5.14.7 修改登录口令

选择菜单**系统工具→修改登录口令**，可以在下图 5-59界面中修改登录路由器管理界面的用户名和密码。修改完成后，点击**保存**按钮即可。

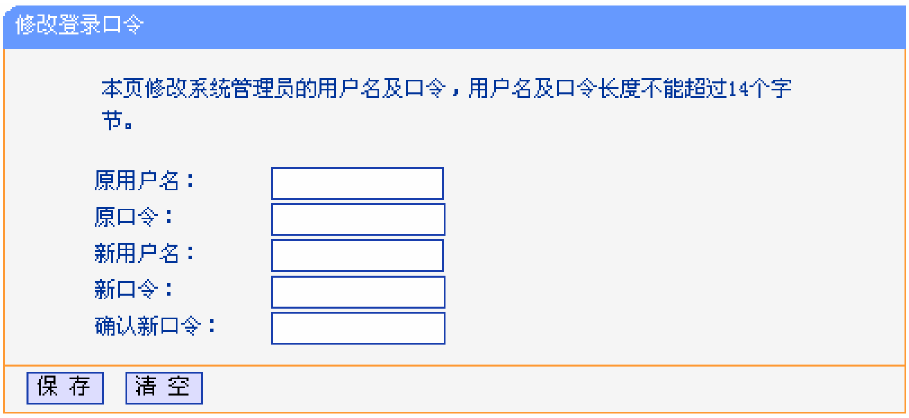


图 5-59 修改登录口令

☞ 注意：

出于安全考虑，我们强烈推荐您更改初始系统管理员的用户名及密码。如果忘了系统密码，请将路由器恢复到出厂设置(如何恢复请参考3.2 复位)。

5.14.8 系统日志

选择菜单**系统工具→系统日志**，可以在下图 5-60中查看路由器的日志信息。该界面记录了路由器的系统日志，可以通过查询日志了解网络情况和快速定位设备故障。



图 5-60 系统日志

刷新： 点击此按钮，路由器将刷新页面，显示最新的日志列表。

清除所有日志： 点击此按钮，路由器中的日志将被永久删除。

5.14.9 流量统计

选择菜单**系统工具→流量统计**，可以在下图 5-61中查看路由器的流量信息。单击**刷新**按钮，可以更新流量统计表；单击路由器数据流量统计表中对应条目后的**重置**，可以将该条目当前的流量数据全部清零，并重新开始统计；单击**删除**，可以删除指定的流量统计信息。



图 5-61 流量统计

数据包统计时间间隔： 该数值决定了统计路由器当前流量的时间间隔。

IP 地址： 被统计主机的 IP 地址，此处也会显示该主机的 MAC 地址。

总流量： 该项分别用数据包个数和字节数来统计路由器接收和发送数据的总流量。

当前流量： 该项显示在不同的统计单位下，路由器在当前 10 秒钟内接收和发送不同数据的总流量。

☞ 注意：

若要查看路由器的流量信息，必须先开启路由器的流量统计功能。如无需流量统计，可以关闭该功能，这样可以提高路由器的数据处理能力。

附录A FAQ

1. 忘记了登录路由器的用户名和密码怎么办（如何将路由器复位）？

忘记了登录路由器的用户名和密码只能将路由器恢复到出厂默认设置，即复位。在路由器的后面板上有一个标识为 **QSS/RESET** 的按钮，通电状态下，按下 **QSS/RESET** 键 5 秒钟，**系统状态指示灯**快速闪烁 3 次后松开，复位成功。

注意：复位后路由器默认登录 IP 为 **192.168.1.1**，默认用户名/密码是 **admin/admin**。登录时，请确保计算机的 IP 地址在 192.168.1.X（X 为 2 到 254 之间的任意整数）网段。

2. 登录不了路由器的管理界面怎么办？

1) 请确保计算机连接在路由器的 1/2/3/4 口的其中一个，并且相应指示灯是亮的；

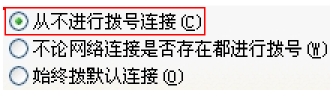
2) 请确认计算机的 IP 地址与路由器登录 IP 地址处于同一网段；如路由器默认登录 IP 地址为 192.168.1.1，则计算机 IP 地址须为 192.168.1.X（X 为 2 到 254 之间的任意整数）；

3) 如果您修改了路由器的 WEB 管理端口（默认为 80），则登录路由器管理界面时应输入 http://LAN 口 IP:端口号，如 http:192.168.1.1:88；

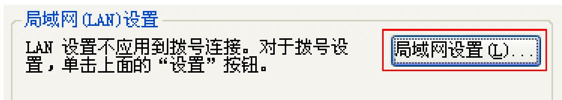
4) 请确保浏览器设置为从“不进行拨号连接”并且没有设置代理服务器；

方法如下（以 IE 浏览器为例）：

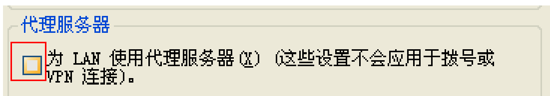
依次选择**工具—Internet 选项—连接**，选择“从不进行拨号连接”：



单击**局域网设置**



如下图设置：



5) 可尝试更换其它计算机进行登录；

若上述提示不能帮助您登录到路由器，请将路由器恢复出厂设置并重新操作。

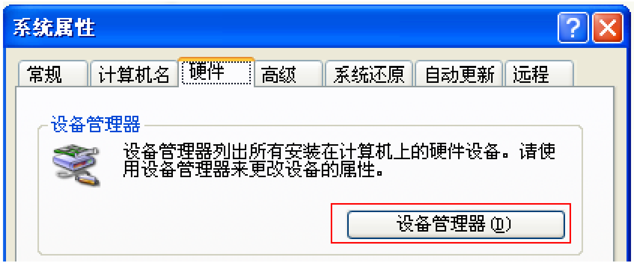
3. 为什么我的笔记本电脑搜索不到无线信号？

1) 如果是笔记本电脑内置的无线网卡，请确认无线功能开关已打开（建议联系笔记本电脑厂商或查阅相关说明书）；

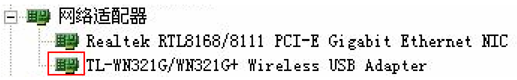
2) 在设备管理器中查看无线网卡驱动是否成功安装以及无线网卡是否已启用；

方法如下：

右键点击桌面上的**我的电脑**，选择**属性-硬件-设备管理器**



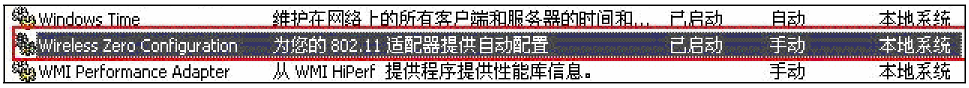
如下图中的绿色标识表示网卡驱动已安装成功且启用



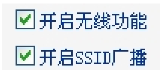
3) 检查笔记本电脑的无线服务是否开启；

方法如下（以 Windows XP 为例）：

右键点击桌面上我的电脑，选择管理。在计算机管理中选择“服务和应用程序”，再在“服务”页面里面查看“Wireless Zero Configuration”的状态。



4) 请确认无线路由器的无线功能已开启且允许 SSID 广播。



5) 尝试近距离是否可以搜索到无线信号，避免因障碍物太多导致信号衰减严重；

若上述提示不能帮助到您，请确认其它的无线网卡是否可以连接到该无线路由器。如果都不可以，请将路由器恢复到出厂设置。

4. 为什么我的笔记本电脑搜到无线信号却连接不上？

1) 请确认尝试连接的无线信号的名称与无线路由器设置的 SSID 号一致；

2) 请确认无线信号的强度，如果信号较弱，建议调整无线路由器的位置或近距离连接；

3) 请确认无线路由器是否设置加密，如果已设置加密，检查无线网卡与无线路由器的加密设置是否一致；

4) 删除电脑上的无线网卡原有配置文件，重新进行连接；

5) 咨询笔记本电脑或无线网卡的厂商，按照相关的指导操作无线网卡进行连接；

若仍然无法连接，请将路由器恢复到出厂设置并重新设置。

5. 如何判断我的上网方式？

一般情况下，我们可以通过如下几种简单的方法来辨别常见的上网方式：

1) ADSL 虚拟拨号（PPPOE）：宽带服务商只提供了一个用户名和密码（帐号和口令），不接路由器时需拨号上网；

2) 静态 IP 地址：宽带服务商提供了相关的 IP 地址和网关等信息，不用路由器时需要配置相关参数才可以上网；

3) 动态 IP 地址：宽带服务商没有提供任何参数，计算机不需要做任何设置。

6. 无线路由器当无线AP（无线交换机）使用，怎么设置？

在现有的有线网络中实现无线功能时，可以把无线路由器当作一个无线 AP（无线交换机）使用，设置步骤如下：

1) 登录无线路由器管理界面，更改无线路由器的 LAN 口 IP 地址，避免与内网其它设备冲突；关闭无线路由器的 DHCP 功能并重启；
2) 将无线路由器的 1/2/3/4 任意一口与有线网络中的路由器或交换机有线连接起来；
3) 将网络中的无线网卡连接到无线路由器；
4) 配置无线网卡的网络参数(自动获取或手动配置，手动配置参数与原先使用有线时一致)；

7. 忘记无线加密的密钥怎么办？

一般来说有以下两种方法：

1) 使用网线连接计算机和无线路由器，通过有线的方式登录无线路由器并查看**无线安全设置**的相关参数；
2) 将无线路由器恢复到出厂设置。

8. 有线使用正常，为什么无线上不了网？

一般情况下，如果使用有线连接可以正常上网，那么说明路由器的配置基本上是正常的。请从下面几个方面排除故障：

1) 检查无线网卡和无线路由器是否连接成功，（即检查用无线方式能否登录路由器管理界面）；
2) 确认连接到了正确的无线路由器（根据 SSID 号判断）；
3) 检查无线网络连接是否配置了正确的 IP 地址、网关和 DNS 服务器地址；
4) 检查一下路由器安全设置中有无设置过滤；

9. 为什么QQ正常，却打不开网页？

1) 检查网络连接是否配置了正确的 DNS 服务器地址（可以咨询当地运营商或者登录路由器的管理界面，在**运行状态—WAN 口状态—DNS 服务器**处查看）；
2) 检查浏览器设置为从不进行拨号连接并且没有设置代理服务器；
3) 更换一个浏览器（如 Firefox）进行访问。

10. 无线信号受哪些因素的影响？

1) 无线局域网采用的是微波传输，微波的最大特点就是绕射能力非常弱。家庭中最主要的障碍物就是墙壁，它不仅阻挡无线信号还能把电磁的能量吸收掉，因此身处在墙后面的无线接收设备只能接到很微弱的信号，或没有收到信号。
2) 微波炉、蓝牙设备、无绳电话、电冰箱等的强大磁场会使无线网络信号受到影响。
3) 如果在无线环境中存在多台无线设备还有可能存在频道冲突，无线信号串扰的问题。
4) 距离无线设备及电缆线路 100 米内的无线电发射塔、电焊机、电车或高压电力变压器等强信号干扰源，也可能会对无线信号或设备产生强干扰。
5) 室外传播时天气情况对无线信号的影响也很大，雷雨天或天气比较阴沉的时候信号衰减比较厉害，晴天里信号能传输的距离会比较远。

11. 如何改善信号传输质量？

1) 为无线路由/AP 选择一个最佳的放置地点。这个放置地点的要求如下：一、位置应偏高一些，以便在较高地方向下辐射，减少障碍物的阻拦，尽量减少信号盲区；二、位置地点选择时应使信号尽量少穿越隔墙，最好使房间中的无线客户端能与无线 AP 可视。另外，放好后可微调路由器或天线的位置，以便找到最佳放置点。

2) 修改频道，减少无线串扰。注意：设置自己无线信号发射频道时也要尽量保证离别人的无线信号频道 5 个以上。

3) 减少居家电器干扰，保证信号畅通无阻。放置无线 AP 时尽量远离上述设备。

4) 如果无线路由/AP 天线是可拆卸的，可以通过更换天线达到增强无线信号的目的。

附录B IE浏览器设置

1 打开 IE 浏览器，选择菜单工具→**Internet 选项…**，如下图 1 所示。



图 1

2 在 Internet 选项界面中点击"连接"，勾选"从不进行拨号连接"，或将"拨号和虚拟专用网络设置"中的设置内容全部删除(即将下图中的"宽带连接（默认）"删除)，如图 2 示。

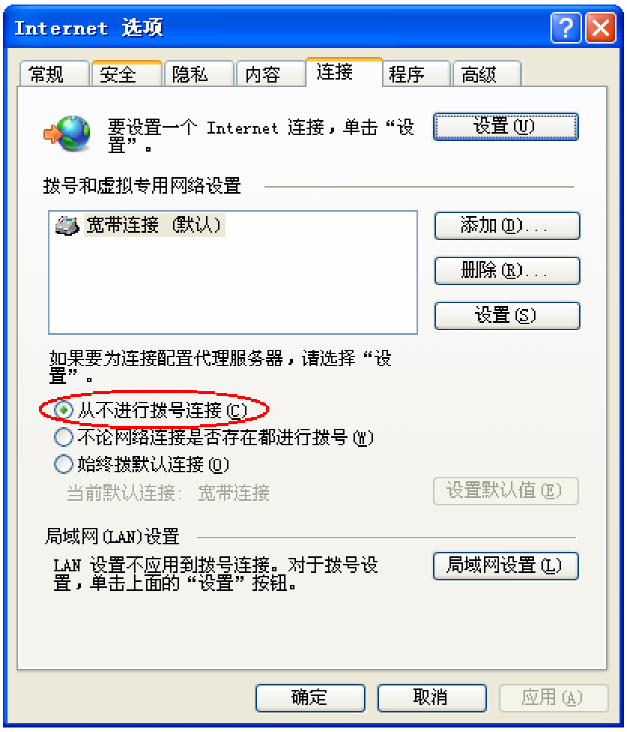


图 2

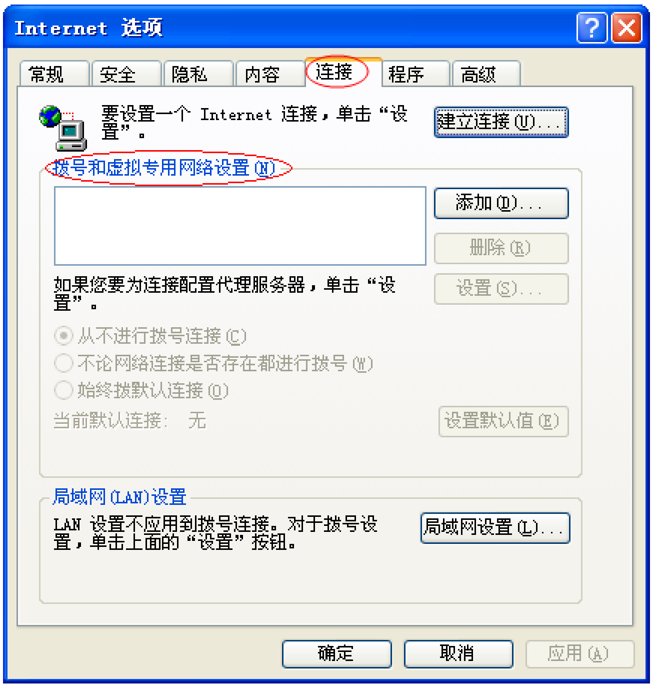


图 3

3　点击图 3 中的**局域网设置...**按钮，确保“代理服务器”下的复选框处于非选中状态，如下图界面所示，单击**确定**按钮返回。

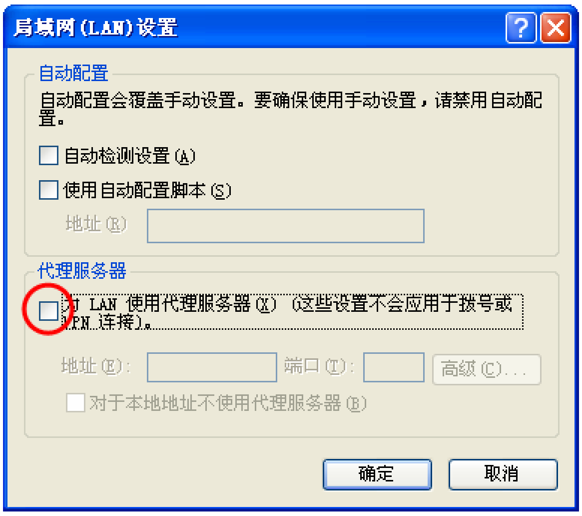


图 4

4　回到 IE 浏览器界面，选择菜单**文件**，单击下拉菜单中的**脱机工作**将该项将前面的“√”去掉，如下图示。若该项前面没有“√”符号则表示脱机工作没有启用，不用设置。

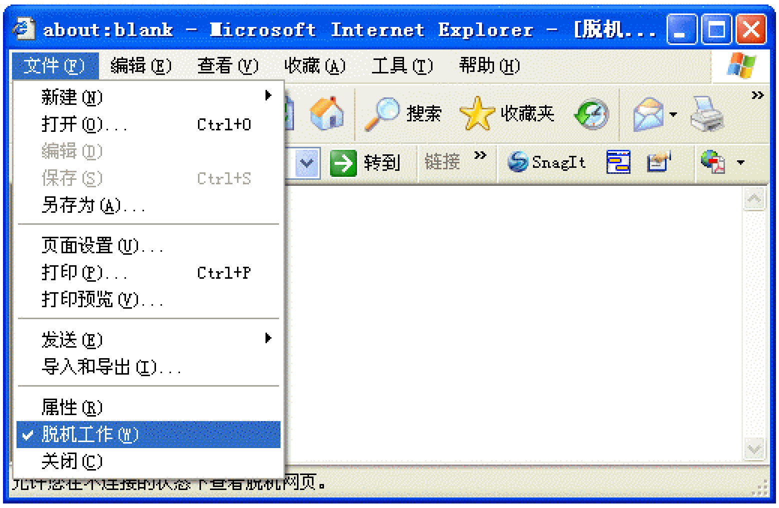

about:blank - Microsoft Internet Explorer - [脱机...
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
新建(N)
打开(O)... Ctrl+O
编辑(D)
保存(S) Ctrl+S
另存为(A)...
页面设置(U)...
打印(P)... Ctrl+P
打印预览(V)...
发送(E)
导入和导出(I)...
属性(R)
脱机工作(W)
关闭(C)
搜索
收藏夹
转到
链接
SnagIt

图 5

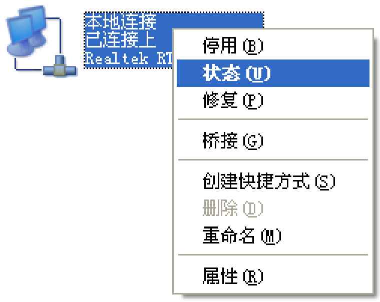
附录C MAC地址查询

一、Windows XP 系统下的查询

1. 右键单击桌面上的“网上邻居”图标，在弹出的快捷菜单中选择**属性**。



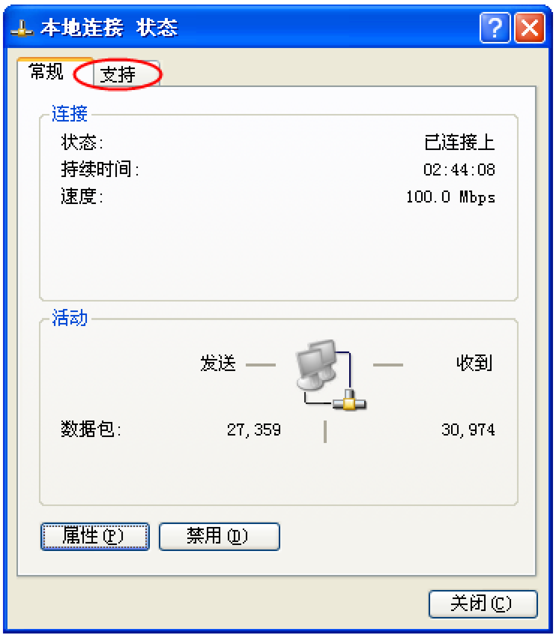
2. 在打开的新页面中，右键单击“本地连接”，选择**状态**。



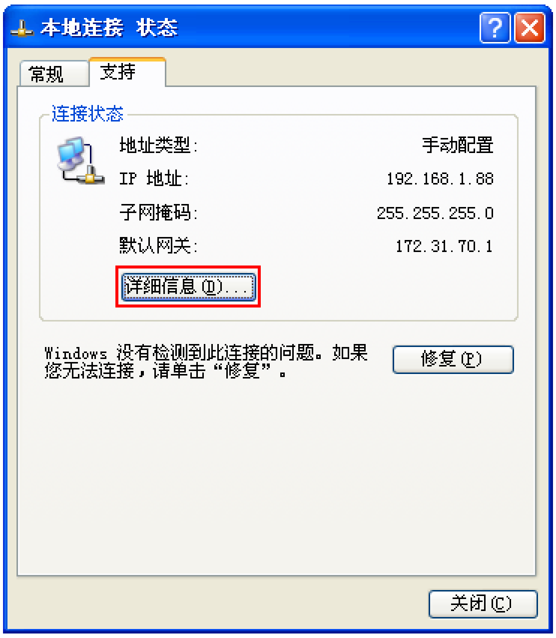
✍ 提示：

也可以在**开始→控制面板→网络和 Internet 连接→网络连接**中找到“本地连接”。

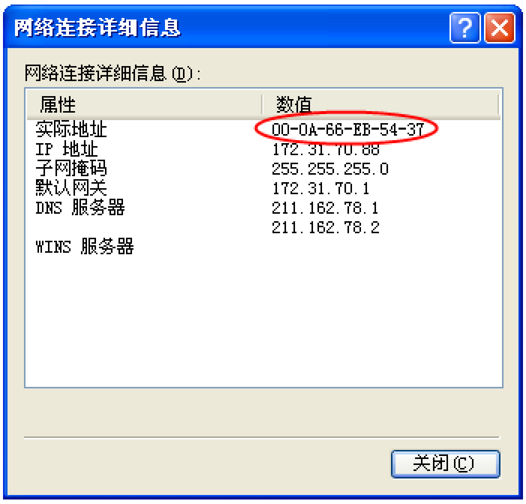
3. 单击“本地连接 状态”页面中的“支持”选项卡。



4. 单击页面中的**详细信息**按钮。



5. 在打开的“网络连接详细信息”页面中，看到的“实际地址”即是当前计算机的 MAC 地址。MAC 地址格式为 XX-XX-XX-XX-XX-XX，其中 X 为 16 进制数，即 0~9 或 A~F 之间的值。此例中查看到的 MAC 地址为 00-0A-66-EB-54-37。



二、**Windows Vista** 系统下的查询

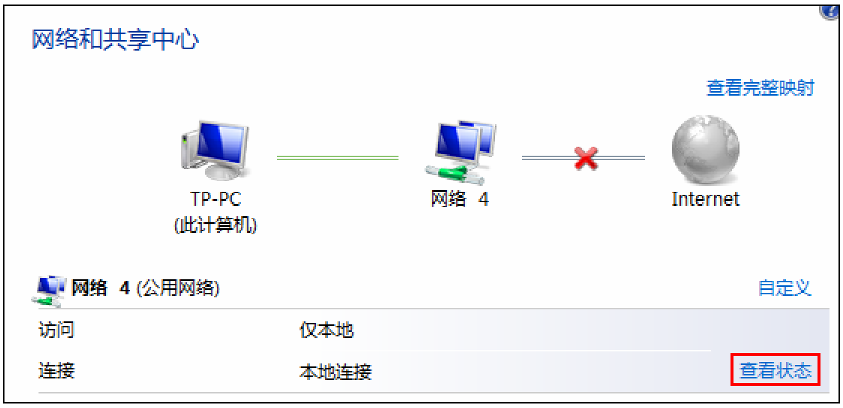
1. 单击任务栏上的**开始**按钮，然后选择“控制面板”。



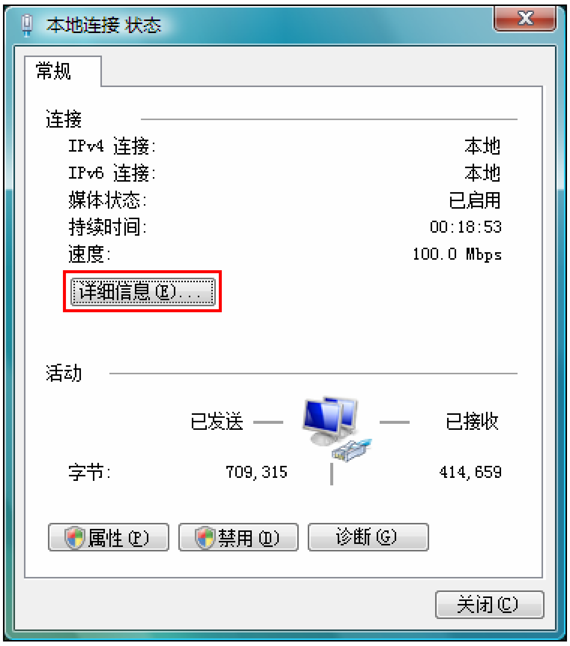
2. 选择页面左边的“经典视图”，然后双击“网络和共享中心”。



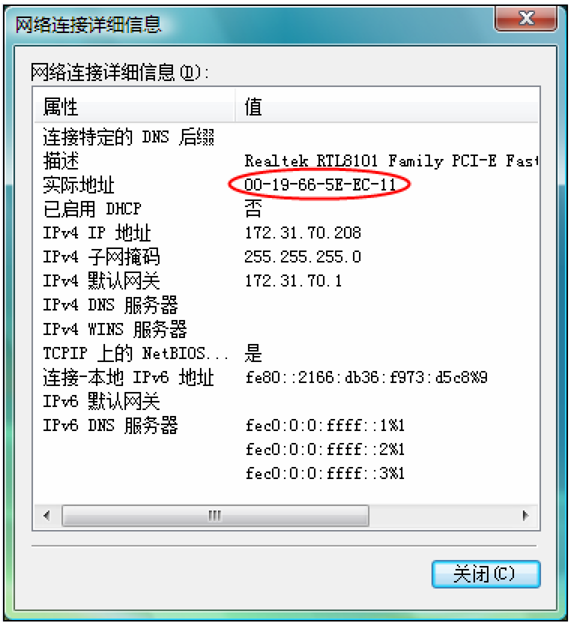
3. 在打开的页面中，单击"查看状态"。



4. 单击"本地连接 状态"页面中的**详细信息**按钮。



5. 在打开的“网络连接详细信息”页面中，您看到的“实际地址”即是当前计算机的 MAC 地址。MAC 地址格式为 XX-XX-XX-XX-XX-XX，其中 X 为 16 进制数，即 0~9 或 A~F 之间的值。此例中查看到的 MAC 地址为 00-19-66-5E-EC-11。



附录D 规格参数

支持的标准和协议		IEEE 802.11g、IEEE 802.11b、IEEE 802.3、IEEE 802.3u、IEEE 802.3x、IEEE 802.1X、CSMA/CA、CSMA/CD、TCP/IP、DHCP、ICMP、NAT、PPPoE
端口	LAN口	4个10/100M自适应RJ45端口(Auto MDI/MDIX)
	WAN口	1个10/100M自适应RJ45端口(Auto MDI/MDIX)
无线参数	频率范围	2.4～2.4835GHz
	传输速率	11n：最高可达150Mbps 11g：6/9/12/18/24/36/48/54Mbps 11b：1/2/5.5/11Mbps
	工作信道数	13
	展频技术	DSSS（直接序列展频）
	数据调制方式	11n：BPSK,QPSK,16-QAM,64-QAM 11g：BPSK,QPSK,16-QAM,64-QAM 11b：CCK,DQPSK,DBPSK
	介质接入协议	CSMA/CA with ACK
	数据加密	WPA/WPA2；64/128/152-WEP；TKIP/AES
	传输功率	18dBm（最大值）
	天线数目	1根
	天线类型	偶极子全向天线
网络介质		10Base-T：3类或3类以上UTP
		100Base-TX：5类UTP
LED指示	端口	(WAN)、 (LAN) （指示各端口的Link/Act状态）
	其它	（系统指示）， （无线状态指示）， (QSS安全连接指示)
外形尺寸(L x W x H)		158mm x 120mm x 34mm
使用环境		工作温度：0ºC 到 40ºC
		存储温度：-40ºC 到 70ºC
		工作湿度：10% 到 90% RH不凝结
		存储湿度：5% 到 90% RH不凝结